No. 16-

IN THE

Supreme Court of the United States

POWER VENTURES, INC. AND STEVEN VACHANI,

Petitioners,

v.

FACEBOOK, INC.,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

THOMAS LEE
Counsel of Record
ANDREW SCHWENK
HUGHES HUBBARD & REED LLP
One Battery Park Plaza
New York, New York 10004
(212) 837-6000
thomas.lee@hugheshubbard.com

Counsel for Petitioners

MARCH 9, 2017

271720

QUESTION PRESENTED

Whether an online company given consent by users of an online social networking service to access data shared or stored by the users on the service, but is prohibited access by the service, "intentionally accesses a computer without authorization . . . and thereby obtains information from [a] protected computer" in violation of 18 U.S.C. § 1030(a)(2)(c) of the Computer Fraud and Abuse Act of 1986.

RULE 29.6 STATEMENT

Petitioner Power Ventures, Inc., states that it has no parent corporation and that no publicly held company owns 10% or more of its stock.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

RULE 29.6 STATEMENT ii

TABLE OF CONTENTS iii

TABLE OF AUTHORITIES vi

OPINIONS BELOW 1

JURISDICTION 1

STATUTORY PROVISIONS INVOLVED 1

STATEMENT OF THE CASE 3

THE PROCEEDINGS BELOW 6

REASONS FOR GRANTING THE PETITION 8

I. THE NINTH CIRCUIT'S INTERPRETATION OF A FEDERAL STATUTE IMPLICATING A QUESTION OF NATIONAL IMPORTANCE IS CLEARLY ERRONEOUS AND SHOULD BE REVERSED. 14

II. THIS COURT SHOULD ALTERNATIVELY GRANT AND CONSOLIDATE WITH THE PENDING PETITION IN *NOSAL* TO GIVE GUIDANCE TO THE CIRCUITS IN CONFLICT OVER THE PROPER INTERPRETATION OF "WITHOUT

AUTHORIZATION" IN 18 U.S.C. § 1030(A)(2)(C) 23

III. THIS CASE IS A FLAWLESS VEHICLE FOR DECIDING THE QUESTION PRESENTED, WHETHER BY GRANTING THIS PETITION OR BY CONSOLIDATION. 26

CONCLUSION 27

TABLE OF APPENDICES

Page

APPENDIX A — ORDER AND AMENDED OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, DATED DECEMBER 9, 2016 ..... 1a

APPENDIX B — ORDER OF THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION, FILED FEBRUARY 16, 2012 ..... 25a

APPENDIX C — ORDER OF THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION, FILED SEPTEMBER 25, 2013 ..... 57a

TABLE OF AUTHORITIES

Page(s)

Cases

Butera & Andrews v. IBM Corp., 465 F. Supp. 2d 104 (D.D.C. 2006) 25

Calence, LLC v. Dimension Data Holdings, 2007 WL 1549495 (W.D. Wash. 2007) 25

Doe v. Dartmouth-Hitchcock Med.l Ctr., 2001 WL 873063 (D.N.H. 2001) 25

EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (CA1 2001) 24

Exxon Mobil Corp v. Allapattah Servs. Inc., 545 U.S. 546 (2005) 13, 26

Gonzaga University v. Doe, 536 U.S. 273 (2002) 10

Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418 (CA7 2006) 24

Musacchio v. United States, 136 S. Ct. 709 (2016) 23

Nosal v. United States, 844 F.3d 1024 (CA9 2016) ..... *passim*

Owasso Ind. Sch. Dist. No. 1-011 v. Falvo, 534 U.S. 426 (2002) 10, 19, 20

SBM Site Servs., LLC. V. Garrett, 2012 WL 628619 (D. Colo. 2012) 25

United States v. John, 597 F.3d 263 (CA5 2010) 9, 24

United States v. Nosal, 676 F. 3d. 854 (CA9 2012) (*en banc*) 11, 24

United States v. Rodriguez, 628 F.3d 1258 (CA11 2010) 24

United States v. Teague, 646 F.3d 1119 (CA8 2011) 9, 24

United States v. Valle, 807 F.3d 508 (CA2 2015) 20, 24

WEC Carolina Energy Sols. v. Miller, 687 F.3d 199 (CA4 2012) 24

White v. Woodall, 134 S. Ct. 1697 (2014) 20

Constitutional Provisions

Fourth Amendment 4

Statutes and Rules

18 U.S.C. 14

18 U.S.C. § 1030 ..... *passim*

28 U.S.C. § 1254(1) 1

28 U.S.C. § 1291 1

28 U.S.C. § 1367 ..... 1, 13, 26

28 U.S.C. § 2254(d)—a 21

California Penal Code § 502 6

Fed. R. Civ. Pro. 20 26

Fed. R. Civ. Pro. 20 and 23 ..... 13, 26

20 U.S.C. § 1232(g) 19, 20

Sup. Ct. R. 10(c) 10, 14

Sup. Ct. R. 12(4) 11, 25

Treatises and Periodical Materials

Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability* (Dec. 13, 2016) 4, 21

Aarti Shahani, *The Man Who Stood Up to Facebook*, NPR (Oct. 13, 2016) 22

Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*" 78 N.Y.U. L. Rev. 1586 (2003) 15

Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016) 23

Orin Kerr, *9th Circuit: It's a Federal Crime to Visit a Website After Being Told Not to Visit It*, Washington Post online (July 12, 2016) 23

Mark Lemley, *Place and Cyberspace*, 91 Calif. L. Rev. 521, 523–26 (2003) 18

Josephine Wolff, *The Hacking Law That Can't Hack It*, Slate.com (Sept. 27, 2016) 22

Power Ventures, Inc., and Steven Vachani respectfully petition this Court to grant a writ of *certiorari* to review the final decision of the U.S. Court of Appeals for the Ninth Circuit entered in this action on December 9, 2016.

OPINIONS BELOW

The Ninth Circuit panel's opinion is reported at 844 F.3d 1058 and is reproduced in Appendix A. The opinion of the District Court granting summary judgment is reported at 844 F. Supp. 2d 1025 and is reproduced in Appendix B. The opinion of the District Court denying reconsideration is unreported and is reproduced in Appendix C.

JURISDICTION

The panel (Graber, Wardlaw, Murguia) entered judgment on July 12, 2016. Petitioners timely filed for panel rehearing and rehearing *en banc*. Rehearing was denied on December 9, 2016; the panel entered an amended final judgment the same day. This Court's jurisdiction is invoked under 28 U.S.C. § 1254(1).

This civil action is one arising under federal law, over which the district court had subject matter jurisdiction under 28 U.S.C. § 1331 and § 1367 (supplemental California law claim). The Ninth Circuit had appellate jurisdiction under 28 U.S.C. § 1291.

STATUTORY PROVISIONS INVOLVED

18 U.S.C. § 1030(a)(2)(c) provides:

"Whoever—intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains—information from any protected computer . . . shall be punished as provided in subsection (c) of this section."

18 U.S.C. § 1030(e) defines key terms including:

> As used in this section –
>
> (1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device
>
> (2) the term "protected computer" means a computer—
>
> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States

18 U.S.C. § 1030(g) provides that:

"Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or equitable relief."

STATEMENT OF THE CASE

Petitioners are Power Ventures, Inc., and Steven Vachani, the CEO of Power Ventures, Inc. (collectively "Power"). From 2006 to 2011, Power operated an online communications, personal data management, and social networking aggregator hosted at the website www.power.com. Power offered registered users the capacity to access multiple online social networks (*e.g.*, LinkedIn, Twitter), messaging services (*e.g.*, Microsoft messenger—MSN), and email accounts (*e.g.*, Google mail) through a single, integrated online interface consisting of a digital dashboard and browser. This online interface also featured popular add-in applications like a unified address book and mailbox integrating all of a user's contacts, emails, social network messages, and instant messages in one place. The interface additionally enabled Power users to move files between different accounts with a click-and-drag function, like a user moves folders on an Apple Computer desktop or in Microsoft Windows. Power attracted more than ten million dollars of investment as a startup from noted Silicon Valley venture capital firms like Draper Fisher Jurvetson (who also invested in Hotmail, Skype, and Tesla) and registered more than twenty million users at its peak.

One key feature Power offered was the ability to transfer document files, address book contacts, in-

stant messages, emails, and photos easily from one online service to another. Because it is so time-consuming for people to move countless bits of data manually from one service provider to a competitor, online companies like Power that facilitate moving a user's data when one provider's terms of use are too onerous are indispensable to lives lived increasingly on line. The right of a user to readily move, copy, and transmit his or her own personal data between online service providers and storage devices is called "data portability." Data portability is a burgeoning policy concern of our time, as underscored by a recent report issued by the European Commission's Directorate General Justice and Consumers. (*See* Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability* (Dec. 13, 2016), *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf).[1]

Respondent Facebook, Inc., is a publicly listed Delaware corporation founded in 2004 and presently headquartered in California. Facebook operates the now-ubiquitous social networking website www.facebook.com. Facebook activates accounts for its users (now numbering nearly two billion worldwide) who register with a unique username and password and agree online to "terms of use." Facebook users send "friend" requests to other friends

[1] Data portability may be seen as the modern digital analogue of the old freedom to dispose freely of one's possessions, papers, and effects, protected from government intrusion by the Fourth Amendment.

with Facebook accounts and post photos, observations, status and event updates, and links to interesting websites and articles for their Facebook friends. Each Facebook user may set the audience to which he or she wishes to post or share data like pictures and updates (*e.g.*, friends only, the public at large), and also the types of friends' updates for which they would like to receive notifications.

In November 2008, Power, which then had over five million users, began offering any user who had a Facebook account access to it through Power's online portal by entering his or her Facebook username and password. When these were entered, the Power user could access the Facebook website through Power's browser, similar to a computer user clicking on his or her programs through Microsoft Windows. (Google, LinkedIn, Microsoft Messenger, Twitter, and Myspace were already accessible via the Power portal in the same way.) Power users were also invited, as part of a launch promotion, to invite their own Facebook friends to enroll on Power via "event" or "status" updates that caused Facebook-generated emails to be sent to Facebook friends whose notifications filters were set to allow them.

Facebook objected that Power's access of its service was unauthorized and sent Power a "cease and desist" letter on December 1, 2008. Power responded that it had the Power users' consent to access data they had stored on Facebook, including their friends' contact information. Facebook insisted, however, that Power join "Facebook Connect," its program for third-party companies or websites to enroll for the right to access user profiles and data on terms that Facebook dictated (*e.g.*, without an easy way to move data). Facebook also unsuccessfully at-

tempted to block Power's IP (internet protocol) address. Settlement negotiations took place during the month of December 2008 but ultimately failed, and Facebook sued. Facebook was the only online social network provider to take legal action against Power. Google, Twitter, Myspace, LinkedIn, Microsoft, and others allowed their users who had Power accounts to access and freely move their personal data among their respective services via Power.

THE PROCEEDINGS BELOW

On December 30, 2008, Facebook filed a civil action against Petitioners in the federal district court for the Northern District of California. Facebook's complaint, which was amended on January 13, 2009, pled claims under the Computer Fraud and Abuse Act of 1986 ("CFAA"), 18 U.S.C. § 1030(a)(2)(C), as well as the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") and California Penal Code Section 502, among others. The statutory provision at issue in this case, 18 U.S.C. § 1030(a)(2)(C), authorizes criminal and civil liability against "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer." The district court granted summary judgment in Facebook's favor on the CFAA, CAN-SPAM and California Penal Code claims. App. 25a. It awarded statutory damages of $3,031,350 under CAN-SPAM, permanent injunctive relief, and held Vachani personally liable for Power's conduct. App. 109a.

Petitioners appealed. In a judgment originally filed July 12, 2016, and amended on December 9,

2016, the Ninth Circuit panel (Graber, Wardlaw, Murguia) reversed the district court on CAN-SPAM and invalidated the damages award (holding that the relevant invitation messages were not misleading). App. 13a, 23a. The appellate court affirmed the district court's ruling on Petitioner Vachani's personal liability. App. 22a. Respondent Facebook did not seek rehearing on the CAN-SPAM reversal, and Petitioners do not challenge the panel's affirmance of personal liability before this Court.

The Ninth Circuit also reversed in part and affirmed in part on the CFAA and California Penal Code claims, and, accordingly, remanded for consideration of appropriate remedies on those claims. App. 23a. The court held that Petitioners had only violated the CFAA (and state law) after Power received the cease-and-desist letter on December 1, 2008 and did not end its marketing campaign via Facebook users. App. 23a-24a. The court reasoned that because the Power users with Facebook accounts had consented to allow Power to access their Facebook contacts, "it did not initially access Facebook's computers 'without authorization' within the meaning of the CFAA." App. 17a. The court asserted, however, that liability under the statute changed after Facebook sent the cease-and-desist letter, regardless of the users' consent that it had held to have constituted "authorization" under the statute before the letter. App. 17a. "The consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission." App. 19a. The court accordingly held that "after receiving written notification from Facebook on December 1, 2008, Power accessed Facebook's comput-

ers 'without authorization' within the meaning of the CFAA and is liable under that statute." App. 20a.

Petitioners filed for panel rehearing and rehearing *en banc*, which was denied on December 9, 2016; the panel issued an amended judgment the same day. App. 1a. Hence this Petition, which seeks this Court's review of the question of CFAA interpretation only.

REASONS FOR GRANTING THE PETITION

Petitioners respectfully submit that the Ninth Circuit's interpretation of 18 U.S.C. § 1030(a)(2)(C) is clearly erroneous and unprecedented. It is unreasonable to conclude as the lower court did that users' consent for Power to access their Facebook data (*i.e.*, friends' photos and contact information) constitutes "authorization" under the CFAA at one point but does not at another. What led the court below to this errant conclusion was the belief that Power was accessing "Facebook's computers" when it reached out to the Facebook friends of Power users with the users' consent and invited them to join Power. But Facebook is not a "protected computer" as the term is defined and used in the 1986 statute: rather, it is a very modern online social network service provider that encourages nearly two billion users worldwide to join it and share personal data with friends and family. In this context, the "authorization" the CFAA refers to is plainly that of the data owners and users. If Facebook wanted Power to stop accessing this data, it could have asked the Power users who owned the data to withdraw the consent they had given to Power, or else cancel the users' accounts.

The Ninth Circuit panel's interpretation of 18 U.S.C. § 1030(a)(2)(C) to ground a private cause of action for an online social network like Facebook as against another online company accessing user data with the user's consent is not only unreasonable, it is unprecedented. Facebook, the party asserting a private right of action under the statute, has no authorship or ownership of the information accessed. Indeed, Facebook's very business model is to entice people—"users"—to share personal information about themselves on its website. This is in stark contrast to prior CFAA private claimants—typically employers or former employers whose computers and databases were hacked for sensitive information. Facebook is not a bank whose account manager pilfered its client-account database to make fraudulent charges, *see United States v. John*, 597 F.3d 263 (CA5 2010), or a government agency whose records (including then President Barack Obama's student loan records) were surreptitiously searched by a government contractor, *see United States v. Teague*, 646 F.3d 1119 (CA8 2011). Rather, Facebook is a digital scrapbook that enables users to curate their own online personae for friends, family, or even the public at large, and the data that Petitioners accessed were these very artifacts of the users' personal lives. Of course, Facebook's proprietary algorithms and confidential business records are its *own* information, and Facebook could surely seek CFAA liability if Petitioners had accessed that information. But that is not this case.

The court below's unreasonable and unprecedented interpretation of the CFAA in this case has immense implications not only in California—home of Silicon Valley, the cradle of modern technological innovation—but also across the nation. Hundreds of

millions (billions, worldwide) of people use Facebook and other social networking and "cloud" storage service providers like LinkedIn, Twitter, Google Docs, Skype, Dropbox, and Microsoft OneDrive to connect with friends and business associates; to store and share cherished photos, stories, and documents; and to post their observations on life's big and small questions. Facebook and other data controllers already have outsized influence over individual users as gatekeepers. Judicial decisions like the one below will aggrandize their power even more by handing them veto power over online entrepreneurs like Petitioners who seek to enable data portability for users.

Additionally, the lower court's interpretation is acutely pernicious because 18 U.S.C. § 1030(a)(2)(C) also grounds criminal liability under the CFAA of up to five years, *ibid.* § 1030(c)(2)(B). If Congress today decides that Petitioners' actions warrant such drastic criminal and civil liability, it can enact a new statute; the Ninth Circuit's creation of such liability by judicial fiat in overreading a 1986 statute is not the right way.

This Court has previously granted *certiorari* when a lower court erroneously interpreted a federal statute on an important national issue, even in the absence of a circuit split. *See, e.g.*, *Owasso Ind. Sch. Dist. No. 1-011 v. Falvo*, 534 U.S. 426 (2002); *cf.* Sup. Ct. R. 10(c) ("an important question of federal law that has not been, but should be, settled by this Court"). *Owasso* is particularly instructive because the Court granted and reversed the lower court's interpretation of a federal statute that it later held in the same Term did not even afford a private right of action. *See Gonzaga University v. Doe*, 536 U.S. 273 (2002).

With special regard to this case, the overwhelming presence of technology companies in California and Washington makes it highly unlikely that a split among the circuits on this precise issue will ripen.[2] Ninth Circuit precedents are often *de facto* the law of the land on cutting-edge social media issues owing to the circuit's hegemony over Silicon Valley.

Alternatively, if this Court were not inclined to grant this Petition as presenting a question of national importance on which it should rule, the Court could hold the Petition over and consolidate it with the soon-to-be pending petition in another Ninth Circuit case, *Nosal v. United States ("Nosal II")*, 844 F.3d 1024 (CA9 2016),[3] for which an extension was filed and granted by this Court until April 7, 2017 (No. 16A840). *Cf.* Sup. Ct. R. 12(4). *Nosal II* is a criminal case involving a charge under 18 U.S.C. § 1030(a)(4), a liability provision of the CFAA with the same "without authorization" language as § 1030(a)(2)(C). It applies to any person who "knowingly and with intent to defraud, accesses a protected

[2] In addition to Facebook, many of the most popular online social media providers like YouTube, Instagram, and Twitter, are based in California. Some of the largest cloud service providers are also in the Ninth Circuit's geographic jurisdiction: Apple, Dropbox, and Google Drive have headquarters in California, and Microsoft and Amazon are based in Washington state.

[3] An earlier case involved some of Nosal's colleagues at Korn/Ferry who downloaded confidential information from their employer in violation of company policies before jumping ship with Nosal to launch a competitive firm. *See United States v. Nosal ("Nosal I")*, 676 F. 3d. 854 (CA9 2012) (*en banc*).

computer without authorization … and by means of such conduct furthers the intended fraud and obtains anything of value." *Ibid.* § 1030(a)(4). Nosal, the defendant, accessed the confidential database of a former employer (the executive recruitment firm Korn/Ferry) by using the password of his former executive assistant who stayed on at Korn/Ferry at his request. The jury convicted Nosal of conspiracy to violate the "without authorization" provision of the CFAA under 18 U.S.C. § 1030(a)(4).

Nosal II and this case present the same issue of whether a third party (here, Petitioners; there, Nosal) who is denied authorization to access data (here, friends' contact information on Facebook; there, Korn/Ferry's confidential database) may do so with the consent of an authorized user (here, Power users with Facebook accounts; there, Nosal's ex-executive assistant). As the dissenting judge pointed out, because *Nosal II* involved a person (the assistant) who had authorization as a continuing Korn/Ferry employee to access its database but not for the "use" of enabling Nosal's conspiracy, it could be framed as implicating a 5-3 split among the circuits over whether "without authorization or exceeds authorized access" in the CFAA covers an impermissible use by an authorized person. *See Nosal II*, 844 F.3d. at 1048, 1048-49 (Reinhardt, dissenting).

Of course, there are also important differences between the Petitioners' novel case involving an online social network and *Nosal II*, which is a traditional case involving access to an employer's or former employer's computers or database. But in light of the similarities, the Court could hold over this Petition, grant the two petitions together and consolidate for argument, and issue a decision that will be

highly instructive to lower courts by distinguishing between the two factual contexts as it deems appropriate. *See, e.g., Exxon Mobil Corp v. Allapattah Servs. Inc.*, 545 U.S. 546 (2005) (simultaneously disposing of petitions from CA1 and CA11 regarding the application of the supplemental jurisdiction statute, 28 U.S.C. § 1367(a), to joinder of plaintiffs in diversity suits under Fed. R. Civ. Pro. 20 and 23, respectively).

In sum, this Court should grant *certiorari* in this case. The lower court's interpretation of the CFAA to extend liability to Petitioners as against a social networking website like Facebook is a question of national importance and is clearly erroneous and unprecedented. If uncorrected, the lower court's ruling will affect hundreds of millions of American (and a couple billion non-American) users of Facebook and other social network and cloud providers. Alternatively, this Court could hold over this petition and consolidate with the petition in *Nosal II*, which implicates a deep split regarding the scope of what "without authorization" means in the CFAA. Regardless of what this Court chooses to do, this case presents a flawless vehicle to decide the Question Presented.[4]

[4] Indeed, this case may arguably be a better vehicle than *Nosal II* because the defendant in that criminal case was also convicted of two counts of trade secret theft in violation of the Economic Espionage Act, 18 U.S.C. §§ 1832 (a). *See Nosal II*, 844 F.3d., at 1041.

I. THE NINTH CIRCUIT'S INTERPRETATION OF A FEDERAL STATUTE IMPLICATING A QUESTION OF NATIONAL IMPORTANCE IS CLEARLY ERRONEOUS AND SHOULD BE REVERSED.

The Ninth Circuit's unreasonable and unprecedented interpretation of 18 U.S.C. § 1030(a)(2)(C) of the CFAA to apply to an online social network service provider seeking to bar another online company acting with users' consent from accessing user data is clearly erroneous and risks mischief on hundreds of millions of internet users. Rule 10(c) of this Court explicitly provides that a lower court's decision of an "important question of federal law that has not been, but should be, settled by this Court" is a factor to be considered in granting *certiorari*. And, as elaborated below, this Court sometimes acts to correct a clearly erroneous interpretation of an important statute by a lower court, even in the absence of a circuit split, to prevent ripple effects or dire national consequences.

The CFAA, 18 U.S.C. § 1030, was initially enacted as part of the Comprehensive Crime Control Act of 1984. *See* Pub. L. No. 98-473, 98 Stat. 1837 (1984). The 1984 statute was substantially revised in 1986, with minor subsequent revisions. The CFAA has both criminal and civil liability provisions, with criminal sentences ranging from twenty years, *e.g.*,18 U.S.C. § 1030(c)(1)(B), to one year, *e.g.*, *ibid.* § 1030(c)(2). The statute's provision for a private right of action states that: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or equitable relief." *Ibid.* § 1030(g). Facebook brought its CFAA claim against Petitioners pursuant to this provision.

The specific provision of the CFAA that Facebook alleged Petitioners had violated was 18 U.S.C. § 1030(a)(2)(C), which provides: "Whoever—intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains—information from any protected computer . . . shall be punished as provided in subsection (c) of this section."[5]

18 U.S.C. § 1030(e)(1) defines "computer" to include not only "data processing devices" but also "any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(2) then defines a "protected computer" to mean a "computer":

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States

[5] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*" 78 N.Y.U. L. Rev. 1586 (2003).

A violation of this provision can result in a criminal sentence of up to five years. *Ibid.* § 1030(c)(2)(B).

Thus, Facebook's CFAA claim, which the Ninth Circuit adopted, was that Petitioners had accessed its website and servers—a "protected computer" under CFAA—and that it did so "without authorization" since Facebook had explicitly told them to desist. On Facebook's view, the authorization of the individual users whose Facebook data Petitioners accessed was irrelevant after Facebook had instructed Petitioners to stop: their authorization was no longer the "authorization" the CFAA required. Specifically, the court reasoned:

> Because Power had at least arguable permission to access Facebook's computers [from Power users with Facebook accounts], it did not initially access Facebook's computers 'without authorization' within the meaning of the CFAA. But Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter to Power on December 1, 2008.

App. 17a.

The lower court's holding is unprecedented and unreasonable. Whatever confusion there was about what constituted "without authorization" among the circuits, *see infra* Part II, no court had held until now that the consent of the individual persons who generated, owned, stored, or shared the relevant data or information was irrelevant to the

"authorization" the statute required.[6] To be sure, if the controller or custodian of the data were a bank or a U.S. government agency, then the argument might seem at least superficially plausible. But in this case, Facebook is an online social network provider, with which people voluntarily *share* personal data and information precisely to disseminate it, not to lock it away in a vault or to submit sensitive information to apply for a government job or benefits. Nor is Facebook claiming that its own proprietary algorithms and business records were the information that Petitioners mined. At the very least, the users' authorization has to matter for something: the Ninth Circuit's decision renders it entirely irrelevant after Facebook denied access to Petitioners and gives Facebook the unitary veto power that it wanted with respect to its competitors like Power.

The obvious truth is that the court below was wrong to conclude the statute is meant to afford a private right of action for an online company with consent from its users to access their personal information shared with another online social networking service when the other service tells the company to stop.[7] In such a case, the company is not "intention-

---

[6] Facebook did not argue below that Petitioners exceeded the users' authorization of access to their data. In other words, there is no dispute that Petitioners acted within the consent provided by users with respect to the users' Facebook accounts.

[7] The court below analogized Petitioners' conduct to a person given permission to access jewelry in a friend's safe deposit box who walks into the bank with a shotgun to whom the bank refuses entry. *See* App. 19a. The analogy is inapt and misleading because Facebook's mission is not to secure the users' "property" (*e.g.*, photos, friends'

Footnote continued

ally access[ing] a computer without authorization or exceed[ing] authorized access" and "thereby obtain[ing] information—from any protected computer" in violation of 18 U.S.C. § 1030(a)(2)(C). It is unsurprising that no other circuit court has reached this conclusion, not only because it is an unreasonable construction of the statutory text, but also because this type of issue about the CFAA is likely to rise most commonly if not exclusively in California and portions of the West Coast within the Ninth Circuit's jurisdiction, where almost all U.S. social network and cloud computing service providers are headquartered.

Furthermore, although the lower court repeatedly referred to Petitioner's access to "Facebook's computers," *e.g.*, App. 5a, 14a, it is debatable whether Facebook and its servers are a "protected computer" for purposes of 18 U.S.C. § 1030(a)(2)(C). The

---

Footnote continued from previous page

contact information) in an online vault, but rather to share it with friends and family and sometimes the public at large. Furthermore, Power did not wield a figurative gun: its user-authorized entry into users' Facebook data was not even arguably coercive or dangerous, as evidenced by the fact that every other online service in Facebook's position (like Google and Microsoft) permitted it. As Judge Wardlaw noted during the oral argument below, physical property analogies are often unhelpful in the online context. *Facebook Inc. v. Power Ventures, Inc., et. al*, Oral Arg., 40:48-41:22, No. 13-17102 (CA9 Dec. 9, 2015), *available at* https://www.youtube.com/watch?v=4QUai3OmkdA; *see also* Mark Lemley, *Place and Cyberspace*, 91 Calif. L. Rev. 521, 523–26 (2003) ("[E]ven a moment's reflection will reveal that the analogy between the Internet and a physical place is not particularly strong.").

statute defines a "protected computer" as a computer or "data storage facility or communications facility" that performs a mission perceived as essential to protect against fraud in the 1980s, such as a computer "exclusively for the use of a financial institution or the United States Government," *see ibid.* §§ 1030(e)(1), 1030(e)(2)(A). True, 18 U.S.C. §1030(e)(2)(B)'s catchall reference to a computer "used in or affecting interstate or foreign commerce or communication" is broadly worded. But a social networking website that users access, primarily to stay in touch with friends and family, is far beyond the government mainframes, bank electronic accounts, and electronic trading exchanges that Congress and President Ronald Reagan envisioned when they passed the CFAA. This kind of vital regulation of the new economy should be ratified by a new Congress, not a Congress three decades ago that could not have even imagined a Facebook or a Google.

The Court has previously granted *certiorari* to correct a clear error in interpreting a federal statute likely to have broad repercussions if uncorrected, even in the absence of a circuit split. For example, in *Owasso Independent School District No. 1-011 v. Falvo*, 534 U.S. 426, there was no conflict among the circuits regarding the relevant question of statutory interpretation. Nevertheless, the Court unanimously reversed the Tenth Circuit's interpretation of the Federal Educational Records and Privacy Act of 1974 ("FERPA"), 20 U.S.C. § 1232(g), to reach student-on-student peer grading and reporting of test scores. The Court reasoned that this interpretation "would impose substantial burdens on teachers across the country." *Ibid.* at 435. "Indeed, the logical consequences of respondent's view are all but unbounded." *Ibid.*

Like the Tenth Circuit's erroneous decision in *Owasso* implicating educational privacy records, the Ninth Circuit's clearly erroneous decision regarding data privacy promises to have substantial adverse ripple effects if not corrected. Its interpretation "would impose substantial burdens," not on teachers, but rather on internet users "across the country" locked into their current social network service or cloud storage providers. Furthermore, internet startups like Petitioners would be constrained from offering services like data aggregation and relocation to enhance user freedom and online diversity. Indeed, the Ninth Circuit's error here is even more egregious because a violation of CFAA, unlike FERPA, can ground criminal liability of up to five years in this case, 18 U.S.C. § 1030(c)(2)(B), as well as private liability. As such, there are additional rule of lenity concerns for reversing the lower court's decision. *Cf. United States v. Valle*, 807 F.3d 508 (CA2 2015) (applying the rule of lenity to construe "authorized access" in CFAA narrowly).

Similarly, in *White v. Woodall*, 134 S. Ct. 1697 (2014), the Court granted *certiorari* and reversed a judgment from the U.S. Court of Appeals for the Sixth Circuit affirming the grant of a habeas petition because the Court determined the lower court had misinterpreted the federal habeas statute. Both the federal district and appellate courts held that the state court's refusal to issue a "no adverse inference from failure to testify" instruction to a jury in a death penalty sentencing hearing violated the defendant's due process rights. *Ibid.* at 1701. This Court explained that the federal habeas statute's "unreasonable application" language is only met when the state court's decision is "objectively unreasonable," *ibid.* at 1702, which the Court held was not

the case. Although the Sixth Circuit's application of the statute did not create a circuit split, this Court nonetheless reversed because the circuit "disregarded the limitations of 28 U.S.C. § 2254(d)—a provision of law that some federal judges find too confining, but that all federal judges must obey." *Ibid* at 1701.

The Ninth Circuit's erroneous decision has immense implications for users of online social media and cloud storage. As users create more online data, data portability among different service providers seeking to keep existing users locked in becomes a growing concern. New European Commission guidelines dictate that users must have "the right to transmit personal data from one data controller to another data controller *without hindrance*." (*See* Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, at 4 (Dec. 13, 2016) (emphasis added) (internal quotation marks omitted), *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf). This ensures that users "can obtain and reuse, but also [] transmit the data they have provided to another service provider." *Ibid.* The Ninth Circuit has created civil and criminal liability for a company seeking to assist users—with their consent—fully to use, enjoy, and move their own data online as they choose.

By way of an example, consider a person who pays a monthly subscription to a hypothetical company called PhotoBook, an online cloud storage service, to organize and access family photos from any computer. Over years of creating and saving photos, the user amasses thousands of photos stored in PhotoBook. Then, because of financial need or practical considerations, the user wishes to transfer those

photos to another service or to a personal computer. The user may seek to hire a company such as Power—a digital mover—to transfer the photos because of a lack of time or technological knowhow. But under the Ninth Circuit's interpretation of the CFAA, PhotoBook may unilaterally deny the moving service access to the user's photos, even with the user's explicit consent. PhotoBook not only gains a power to lock-in its users (subject to increasingly onerous terms), it stifles innovation in the internet economy, all based on a clever but erroneous spin on a 1986 statute.

The importance of the Question Presented is underscored by the attention paid to it. The Electronic Frontier Foundation ("EFF"), a prominent internet rights non-profit organization, filed two amicus briefs at different stages of the district court proceedings. In the Ninth Circuit, the EFF again filed two amicus briefs. The latter of which, joined by the national American Civil Liberties Union ("ACLU") and the ACLU of Northern California, explained that the Ninth Circuit's decision risks creating liability for individual internet users, researchers, and journalists. *See* Amicus Brief of EFF et al., No. 13-17154, Dkt. 89 (CA9 Aug. 19, 2016), *available at* https://www.eff.org/document/facebook-v-power-ventures-eff-aclu-amicus-brief. The case and the Petitioners have been the subject of articles in major news organs like NPR, (Aarti Shahani, *The Man Who Stood Up to Facebook*, NPR (Oct. 13, 2016) *available at* https://goo.gl/UAXhVk), Slate, (Josephine Wolff, *The Hacking Law That Can't Hack It*, Slate.com (Sept. 27, 2016), *available at*

https://goo.gl/iXnxey), and by Professor Orin Kerr,[8] in the Washington Post online, (Orin Kerr, *9th Circuit: It's a Federal Crime to Visit a Website After Being Told Not to Visit It*, Washington Post online (July 12, 2016) *available at* https://goo.gl/rdc2Cu).

II. THIS COURT SHOULD ALTERNATIVELY GRANT AND CONSOLIDATE WITH THE PENDING PETITION IN *NOSAL* TO GIVE GUIDANCE TO THE CIRCUITS IN CONFLICT OVER THE PROPER INTERPRETATION OF "WITHOUT AUTHORIZATION" IN 18 U.S.C. § 1030(A)(2)(C)

The meaning of the words "without authorization or exceeds authorized access" in 18 U.S.C. § 1030(a)(2)(C) has sparked conflict among the lower courts and is ripe for guidance from this Court.[9] 18 U.S.C. § 1030(e)(6) defines "exceed authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter."

---

[8] Professor Kerr, a national expert on computer crime law issues, was joint counsel for Petitioners at the court below. *See also* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016).

[9] Last term, in *Musacchio v. United States*, 136 S. Ct. 709 (2016), this Court unanimously held that an erroneous jury instruction on 18 U.S.C. § 1030(a)(2)(C)—that the defendant had to have acted "without authorization *and* exceed authorized access"—did not offend due process, since it presented a tougher standard for conviction than the correct reading of the statute with a disjunctive "or". That decision, accordingly, did not address circuit conflict about the meaning of "without authorization" and "exceeded authorized access."

Because most CFAA cases arise in the context of an employee or ex-employee accessing an employer's computers or database, this definition would appear to foreclose civil and criminal liability in cases where the employee was entitled to access but did so for an unauthorized use. Three circuits have hewed to this narrow definition. *See United States v. Valle,* 807 F.3d 508 (CA2 2015) (New York City policeman not criminally liable for accessing criminal database for personal reasons); *WEC Carolina Energy Sols. v. Miller*, 687 F.3d 199 (CA4 2012); *United States v. Nosal* ("*Nosal I*"), 676 F.3d 854 (CA9 2012).

On the other hand, five circuits have held that employees or ex-employees who access computers to obtain data they have a right to access, but do so for an improper use or do so in violation of the employer's policies, violate the CFAA. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (CA1 2001) (former employee violated CFAA by using "scraper" technology to get price data from a former employer's public website); *United States v. John*, 597 F.3d 263 (CA5 2010); *Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418 (CA7 2006); *United States v. Teague*, 646 F.3d 1119 (CA8 2011); *United States v. Rodriguez*, 628 F.3d 1258 (CA11 2010). This Court has not resolved this 5-3 circuit split between the narrow "no liability for improper use" view and broad "liability for improper use" views of the CFAA.

As described in detail above, the soon-to-be pending petition for *certiorari* in *Nosal II* can be framed as implicating this deep split, and, also, the same issue as this case when framed at a higher level of abstraction. This could be done, for example, by tweaking the Question Presented by this Petition to read: "Whether a third party given consent by a user

to access data on a 'protected computer' acts 'without authorization' in violation of 18 U.S.C. § 1030(a) of the Computer Fraud and Abuse Act of 1986."

Without speaking to the merits of *Nosal II*, Petitioners assert that this case independently warrants grant of *certiorari* because it presents a unique question of national importance about the applicability of the CFAA to online social media companies. This question has ramifications for hundreds of millions, if not billions, of internet users and burgeoning concerns about data portability. In this respect, it differs from the traditional CFAA cases in the lower courts involving access to an employer's or former employer's computers or database, which are usually fact-bound to the specifics of each case of less universal concern.

But if this Court were not inclined to grant this Petition, then Petitioners respectfully request that it hold the Petition over and consolidate it with the soon-to-be pending petition in *Nosal II*, for which an extension was filed and granted by this Court until April 7, 2017. *See Nosal v. U.S.*, No. 16A840 (Feb. 24, 2017); *Cf.* Sup. Ct. R. 12(4). On prior occasions, this Court has done so, to the profit and guidance of lower courts conflicted in similar but not identical applications of an enigmatic statute.[10] For instance,

[10] In fact, there is yet another burgeoning split among the lower courts regarding 18 U.S.C. § 1030(a)(2)(C). One federal district court has held that the new employer of a person who hacks into the computer of a former employer may also be liable under the CFAA. *See SBM Site Servs., LLC. V. Garrett*, 2012 WL 628619 (D. Colo. 2012). Three district courts have held that a new employer under these circumstances cannot be vicariously liable. *See Calence, LLC v. Dimen-*

Footnote continued

in *Exxon Mobil Corp v. Allapattah Servs. Inc.*, 545 U.S. 546 (2005), this Court issued a single opinion construing the supplemental jurisdiction statute, 28 U.S.C. § 1367, with respect to two different factual contexts involving the statute's application to complete diversity and amount-in-controversy requirements for class actions (Fed. R. Civ. Pro. 23) and simple joinder of plaintiffs (Fed. R. Civ. Pro. 20). The Court's decision in *Exxon Mobil* supplied welcome repose to lower courts and lawyers mired for decades in confusion about the statute's meaning. So, too, in the present case, any guidance from this Court on the application of the CFAA's "without authorization" language to different factual contexts such as in this case and *Nosal II* would be illuminating and welcome.

III. THIS CASE IS A FLAWLESS VEHICLE FOR DECIDING THE QUESTION PRESENTED, WHETHER BY GRANTING THIS PETITION OR BY CONSOLIDATION.

The facts relevant to this petition as articulated by the court below are undisputed and sharply frame the crucial question of statutory interpretation raised. Accordingly, the Court will be able to reach and decide the Question Presented without the risk

---

Footnote continued from previous page

sion Data Holdings, 2007 WL 1549495 (W.D. Wash. 2007); *Butera & Andrews v. IBM Corp.*, 465 F. Supp. 2d 104 (D.D.C. 2006); *Doe v. Dartmouth-Hitchcock Med.l Ctr.*, 2001 WL 873063 (D.N.H. 2001).

of an intervening disputed fact or procedural default. The challenged part of the decision below rests entirely on the Ninth Circuit's errant interpretation of 18 U.S.C. § 1030(a)(2)(C). The issue presented here was fully briefed and considered by the Court of Appeals in a reasoned opinion, and so this Court has the benefit of the Court of Appeals' views on the subject. The Question Presented by this Petition has generated national attention and implicates the future of data privacy and portability. It is ripe for a decision by this Court. Given that the lower court's decision on a question of national importance was clearly erroneous and unprecedented, this Court could summarily grant, reverse, and remand. But if the Court is disinclined to do so, Petitioners stand ready to brief and argue the merits of the case before the Court at its pleasure.

CONCLUSION

For the reasons set forth above, this Petition for a Writ of Certiorari should be granted.

Respectfully submitted,

Thomas Lee
Counsel of Record
Hughes Hubbard & Reed LLP
One Battery Park Plaza
New York, New York 10004
(212) 837-6000

APPENDIX

APPENDIX A — ORDER AND AMENDED OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, DATED DECEMBER 9, 2016

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 13-17102

D.C. No. 5:08-cv-05780-LHK

FACEBOOK, INC., A DELAWARE CORPORATION,

Plaintiff-Appellee,

v.

POWER VENTURES, INC., DBA POWER.COM, A CALIFORNIA CORPORATION; POWER VENTURES, INC., A CAYMAN ISLAND CORPORATION,

Defendants,

and

STEVEN SURAJ VACHANI, AN INDIVIDUAL,

Defendant-Appellant.

Appendix A

No. 13-17154

D.C. No. 5:08-cv-05780-LHK

FACEBOOK, INC., A DELAWARE CORPORATION,

Plaintiff-Appellee,

v.

POWER VENTURES, INC., DBA POWER.COM,
A CALIFORNIA CORPORATION,

Defendant,

and

POWER VENTURES, INC., A CAYMAN ISLAND
CORPORATION; AND STEVEN SURAJ VACHANI,
AN INDIVIDUAL,

Defendants-Appellants.

Appeals from the United States District Court
for the Northern District of California
Lucy H. Koh, District Judge, Presiding

Argued and Submitted December 9, 2015
San Francisco, California

Filed July 12, 2016
Amended December 9, 2016

Appendix A

ORDER AND AMENDED OPINION

Before: Susan P. Graber, Kim McLane Wardlaw, and Mary H. Murguia, Circuit Judges.

Opinion by Judge Graber.

SUMMARY*

CAN-SPAM Act / Computer Fraud

The panel filed an order denying a petition for panel rehearing and rehearing *en banc* and amending its opinion affirming in part and reversing and vacating in part the district court's summary judgment in favor of Facebook, Inc., on Facebook's claims against Power Ventures, Inc., a social networking company that accessed Facebook users' data and initiated form e-mails and other electronic messages promoting its website.

Reversing in part, the panel held that Power's actions did not violate the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, or CAN-SPAM Act, which grants a private right of action for a provider of Internet access service adversely affected by the transmission, to a protected computer, of a message that contains, or is accompanied by, header information that is materially false or materially misleading. The panel held that here, the transmitted messages were not materially misleading.

---

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

Appendix A

Reversing in part and affirming in part, the panel held that Power violated the Computer Fraud and Abuse Act of 1986, or CFAA, which prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use, and California Penal Code § 502, but only after it received a cease and desist letter from Facebook and nonetheless continued to access Facebook's computers without permission. With regard to authorization, the panel stated that a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. The panel also stated that a violation of the terms of use of a website, without more, cannot be the basis for liability under the CFAA.

The panel vacated the district court's awards of injunctive relief and damages and remanded for consideration of appropriate remedies under the CFAA and § 502.

ORDER

The opinion filed July 12, 2016, and published at 828 F.3d 1068, is amended by the opinion filed concurrently with this order.

With these amendments, the panel has voted to deny the petition for panel rehearing and rehearing *en banc*.

Appendix A

The full court has been advised of the petition for rehearing *en banc*, and no judge of the court has requested a vote on it.

The petition for panel rehearing and rehearing *en banc* is **DENIED**. No further petitions for panel rehearing or rehearing *en banc* shall be entertained.

OPINION

GRABER, Circuit Judge:

One social networking company, Facebook, Inc., has sued another, Power Ventures, Inc., over a promotional campaign. Power accessed Facebook users' data and initiated form e-mails and other electronic messages promoting its website. Initially, Power had implied permission from Facebook. But Facebook sent Power a cease and desist letter and blocked Power's IP address; nevertheless Power continued its campaign. Facebook alleges that Power's actions violated the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), the Computer Fraud and Abuse Act of 1986 ("CFAA"), and California Penal Code section 502. We hold that Power did not violate the CAN-SPAM Act because the transmitted messages were not materially misleading. We also hold that Power violated the CFAA and California Penal Code section 502 only after it received Facebook's cease and desist letter and nonetheless continued to access Facebook's computers without permission. Accordingly, we affirm in part, reverse in part, and remand to the district court.

Appendix A

BACKGROUND

Defendant Power Ventures, a corporation founded and directed by CEO Steven Vachani, who also is a defendant here, operated a social networking website, Power.com. The concept was simple. Individuals who already used other social networking websites could log on to Power.com and create an account. Power.com would then aggregate the user's social networking information. The individual, a "Power user," could see all contacts from many social networking sites on a single page. The Power user thus could keep track of a variety of social networking friends through a single program and could click through the central Power website to individual social networking sites. By 2008, the website had attracted a growing following.

Plaintiff Facebook also operates a social networking website, Facebook.com. Facebook users, who numbered more than 130 million during Power's promotional campaign, can create a personal profile—a web page within the site—and can connect with other users. Facebook requires each user to register before accessing the website and requires that each user assent to its terms of use. Once registered, a Facebook user can create and customize her profile by adding personal information, photographs, or other content. A user can establish connections with other Facebook users by "friending" them; the connected users are thus called "friends."

Facebook has tried to limit and control access to its website. A non-Facebook user generally may not use the

website to send messages, post photographs, or otherwise contact Facebook users through their profiles. Instead, Facebook requires third-party developers or websites that wish to contact its users through its site to enroll in a program called Facebook Connect. It requires these third parties to register with Facebook and to agree to an additional Developer Terms of Use Agreement.

In December 2008, Power began a promotional campaign to attract more traffic to its website; it hoped that Facebook users would join its site. Power placed an icon on its website with a promotional message that read: "First 100 people who bring 100 new friends to Power.com win $100." The icon included various options for how a user could share Power with others. The user could "Share with friends through my photos," "Share with friends through events," or "Share with friends through status." A button on the icon included the words "Yes, I do!" If a user clicked the "Yes, I do!" button, Power would create an event, photo, or status on the user's Facebook profile.

In many instances, Power caused a message to be transmitted to the user's friends within the Facebook system. In other instances, depending on a Facebook user's settings, Facebook generated an e-mail message. If, for example, a Power user shared the promotion through an event, Facebook generated an e-mail message to an external e-mail account from the user to friends. The e-mail message gave the name and time of the event, listed Power as the host, and stated that the Power user was inviting the recipient to this event. The external e-mails were form e-mails, generated each time that a Facebook

user invited others to an event. The "from" line in the e-mail stated that the message came from Facebook; the body was signed, "The Facebook Team."

On December 1, 2008, Facebook first became aware of Power's promotional campaign and, on that same date, Facebook sent a "cease and desist" letter to Power instructing Power to terminate its activities. Facebook tried to get Power to sign its Developer Terms of Use Agreement and enroll in Facebook Connect; Power resisted. Facebook instituted an Internet Protocol ("IP") block in an effort to prevent Power from accessing the Facebook website from Power's IP address. Power responded by switching IP addresses to circumvent the Facebook block. Through this period, Power continued its promotion even though it acknowledged that it took, copied, or made use of data from Facebook.com without Facebook's permission.

Power's campaign lasted less than two months. On December 20, 2008, Facebook filed this action. Toward the end of January 2009, Power ended its campaign. In April 2011, Power ceased doing business altogether. In total, more than 60,000 external e-mails promoting Power were sent through the Facebook system. An unknown number of internal Facebook messages were also transmitted.

In this action, Facebook alleged violations of the CFAA, the CAN-SPAM Act, and California Penal Code section 502 and moved for summary judgment. The district court granted summary judgment to Facebook on all three claims. The district court awarded statutory

damages of $3,031,350, compensatory damages, and permanent injunctive relief, and it held that Vachani was personally liable for Power's actions. Discovery disputes persisted after the judgment; a magistrate judge ordered Power to pay $39,796.73 in costs and fees for a renewed Federal Civil Procedure Rule 30(b)(6) deposition. Power filed a motion for reconsideration, which the district court denied. Defendants timely appeal both the judgment and the discovery sanctions.

STANDARD OF REVIEW

We review de novo a grant of summary judgment. *Johnson v. Poway Unified Sch. Dist.*, 658 F.3d 954, 960 (9th Cir. 2011). We may affirm the judgment on any ground supported by the record and presented to the district court. *Venetian Casino Resort L.L.C. v. Local Joint Exec. Bd.*, 257 F.3d 937, 941 (9th Cir. 2001).

DISCUSSION

A. CAN-SPAM Act

The CAN-SPAM Act grants a private right of action for a "provider of Internet access service adversely affected by a violation of section 7704(a)(1) of this title." 15 U.S.C. § 7706(g)(1). In relevant part, § 7704(a)(1) makes it unlawful for "any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading."

Appendix A

The CAN-SPAM Act "does not ban spam outright, but rather provides a code of conduct to regulate commercial e-mail messaging practices." *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1047-48 (9th Cir. 2009). To prove a violation of the statute, Facebook cannot simply identify excessive electronic messages. Rather, assuming all facts in favor of the non-moving party, the offending messages must be "materially false" or "materially misleading." 15 U.S.C. § 7704(a)(1).

The statute provides that

> the term "materially," when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

Id. § 7704(a)(6). A "from" line "that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading." *Id.* § 7704(a)(1)(B). And, further, "header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address

the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading." *Id.* § 7704(a)(1)(A).

Here, two types of messages might rise to the level of "materially misleading" under the CAN-SPAM Act: external e-mails sent when Power caused a Facebook event to be created and internal Facebook messages authored by Power that Power users transmitted to their Facebook friends.

We first consider the external e-mails. Facebook generated these e-mails whenever a Power user created a Facebook event, promoting Power. The "from" line of the e-mails identified "Facebook" as the sender. The body was signed "Thanks, The Facebook Team." The header stated that a friend of the recipient invited her to an event entitled "Bring 100 friends and win 100 bucks!"

Because the statute provides that a "from" line that accurately identifies a person who initiated the message is not misleading, it is relevant whether Facebook, identified in the from line, initiated the messages. The statute defines "initiate" as "to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message." *Id.* § 7702(9). It provides that "more than one person may be considered to have initiated a message." *Id.* A Power user gave Power permission to share a promotion, Power then accessed that user's Facebook data, and Facebook crafted and caused

form e-mails to be sent to recipients. These actions all go beyond the routine conveyance of a message. All the actions require some affirmative consent (clicking the "Yes, I do!" button) or some creative license (designing the form e-mails). Because more than one person may be considered to have initiated the message, we hold that, within the meaning of the statute, Power's users, Power, *and* Facebook all initiated the messages at issue.

Because Facebook (among others) initiated the messages, the "from" line accurately identified a person who initiated the messages. Accordingly, the "from" line is not misleading within the meaning of the statute. Similar reasoning also leads us to conclude that the header is technically accurate. Because a Power user consented to share Power's promotion through an event invitation, a header line that stated that a recipient's friend "invited" the recipient to the event does not conceal or misstate a creator of the e-mail.

It is true that the CAN-SPAM Act includes as materially misleading a technically accurate header that includes information accessed through false or fraudulent pretenses or representations. *Id.* § 7704(a)(1)(A). But Power users consented to Power's access to their Facebook data. In clicking "Yes, I do!," users gave Power permission to share its promotion through event invitations. On this record, Power did not use false pretenses or fraudulent representations to obtain users' consent. Therefore, the external messages were not materially misleading within the meaning of the CAN-SPAM Act.

We next consider internal messages sent within the Facebook system. We can find these messages misleading only if they impaired the ability of the recipient to "respond to a person who initiated the electronic mail message" or the ability of Facebook to locate the initiator of the messages. *Id.* § 7704(a)(6). Two factors convince us that the messages are not misleading under this standard. First, the body of the messages included both Power's name and a link to the Power website. A reasonable recipient could understand that Power had drafted the message or had some part in its construction. Second, Facebook users who were identified as the senders did authorize the sending of these messages. It was not misleading for such users to be identified in internal messages sent through the Facebook system.

Because neither e-mails nor internal messages sent through Power's promotional campaign were materially misleading, Power did not violate the CAN-SPAM Act. We reverse the district court on this claim and remand for entry of judgment in favor of Defendants.

B. CFAA

The CFAA prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use. It creates criminal and civil liability for whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). "The statute thus provides two ways of committing the crime of improperly accessing a protected

computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Musacchio v. United States*, 136 S. Ct. 709, 713, 193 L. Ed. 2d 639 (2016). The CFAA provides a private right of action for "[a]ny person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g).

First, we hold that Facebook suffered a loss within the meaning of the CFAA. The statute permits a private right of action when a party has suffered a loss of at least $5,000 during a one-year period. *Id.* § 1030(c)(4)(A)(i)(I). The statute defines "loss" to mean "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). It is undisputed that Facebook employees spent many hours, totaling more than $5,000 in costs, analyzing, investigating, and responding to Power's actions. Accordingly, Facebook suffered a loss under the CFAA.

We next consider whether Power accessed Facebook's computers knowing that it was not authorized to do so. We have previously considered whether a defendant has accessed a computer "without authorization" or in a manner that "exceeds authorized access" under the CFAA.

In *LVRC Holdings LCC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), an employee logged onto his employer's computer, accessed confidential information, and sent e-mails from the computer to himself and his wife with the intention of starting a competing business. We held that a person is "without authorization" under the CFAA "when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id.* at 1135. Because the employee had sent e-mails while he still had authorized access to the company's computers, his actions did not constitute unauthorized use and did not run afoul of the CFAA. *Id.* That fact was key; had the employee accessed company computers without express permission, he would have violated the CFAA. "[I]f [the employee had] accessed LVRC's information on the LOAD website after he left the company in September 2003, [the employee] would have accessed a protected computer 'without authorization' for purposes of the CFAA." *Id.* at 1136.

In *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*) ("*Nosal I*"), a criminal case, we considered whether a group of employees who logged on to a work computer, downloaded information from a confidential database, and transferred it to a competing business "exceed[ed] authorized access." *Id.* at 856. Wary of creating a sweeping Internet-policy mandate, we applied the rule of lenity to the CFAA and reversed liability for the defendant. *Id.* at 863. The decision broadly described the application of the CFAA to websites' terms of service.

"Not only are the terms of service vague and generally unknown . . . but website owners retain the right to change the terms at any time and without notice." *Id.* at 862. As a result, imposing criminal liability for violations of the terms of use of a website could criminalize many daily activities. Accordingly, "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly." *Id.* at 863.

From those cases, we distill two general rules in analyzing authorization under the CFAA. First, a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. Second, a violation of the terms of use of a website—without more—cannot establish liability under the CFAA.[1] Our analysis also is consistent with *United States v. Nosal*, 828 F.3d 865 (9th Cir. 2016) ("*Nosal II*").

Here, initially, Power users arguably gave Power permission to use Facebook's computers to disseminate messages. Power reasonably could have thought that consent from *Facebook users* to share the promotion was

1. One can imagine situations in which those two principles might be in tension—situations in which, for example, an automatic boilerplate revocation follows a violation of a website's terms of use—but we need not address or resolve such questions on the stark facts before us.

permission for Power to access *Facebook's* computers.[2] In clicking the "Yes, I do!" button, Power users took action akin to allowing a friend to use a computer or to log on to an e-mail account. Because Power had at least arguable permission to access Facebook's computers, it did not initially access Facebook's computers "without authorization" within the meaning of the CFAA.

But Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter to Power on December 1, 2008. Facebook's cease and desist letter informed Power that it had violated Facebook's terms of use and demanded that Power stop soliciting Facebook users' information, using Facebook content, or otherwise interacting with Facebook through automated scripts.[3] Facebook then imposed IP blocks in an effort to prevent Power's continued access.

---

2. Because, initially, Power users gave Power permission to use Facebook's computers to disseminate messages, we need not decide whether websites such as Facebook are presumptively open to all comers, unless and until permission is revoked expressly. *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1163 (2016) (asserting that "websites are the cyber-equivalent of an open public square in the physical world").

3. The mention of the terms of use in the cease and desist letter is not dispositive. Violation of Facebook's terms of use, without more, would not be sufficient to impose liability. *Nosal I*, 676 F.3d at 862-63. But, in addition to asserting a violation of Facebook's terms of use, the cease and desist letter warned Power that it may have violated federal and state law and plainly put Power on notice that it was no longer authorized to access Facebook's computers.

The record shows unequivocally that Power knew that it no longer had authorization to access Facebook's computers, but continued to do so anyway. In requests for admission propounded during the course of this litigation, Power admitted that, after receiving notice that its use of or access to Facebook was forbidden by Facebook, it "took, copied, or made use of data from the Facebook website *without Facebook's permission* to do so." (Emphasis added; capitalization omitted.) Contemporaneously, too, soon after receiving the cease and desist letter, Power's CEO sent an e-mail stating: "[W]e need to be prepared for Facebook to try to block us and the [sic] turn this into a national battle that gets us huge attention." On December 4, 2008, a Power executive sent an e-mail agreeing that Power engaged in four "prohibited activities"[4]; acknowledging that Power may have "intentionally and without authorization interfered with [Facebook's] possessory interest in the computer system," while arguing that the "***unauthorized use***" did not cause damage to Facebook; and noting additional federal and state statutes that Power "may also be accused of violating," beyond those listed in Facebook's cease and desist letter. E-mails sent later in December 2008 discussed the IP blocks that Facebook had imposed and the measures that Power took to evade them. Nevertheless, Power continued to access Facebook's data and computers without Facebook's permission.

---

4. The activities were: "- Using a person's Facebook account without Facebook's authorization; - Using automated scripts to collect information from their site; - Incorporating Facebook's site in another database[; and] - Using Facebook's site for commercial purposes[.]"

The consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission. An analogy from the physical world may help to illustrate why this is so. Suppose that a person wants to borrow a friend's jewelry that is held in a safe deposit box at a bank. The friend gives permission for the person to access the safe deposit box and lends him a key. Upon receiving the key, though, the person decides to visit the bank while carrying a shotgun. The bank ejects the person from its premises and bans his reentry. The gun-toting jewelry borrower could not then reenter the bank, claiming that access to the safe deposit box gave him authority to stride about the bank's property while armed. In other words, to access the safe deposit box, the person needs permission *both* from his friend (who controls access to the safe) *and* from the bank (which controls access to its premises). Similarly, for Power to continue its campaign using Facebook's computers, it needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers). Permission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter.

In sum, as it admitted, Power deliberately disregarded the cease and desist letter and accessed Facebook's computers without authorization to do so. It circumvented IP barriers that further demonstrated that Facebook had rescinded permission for Power to access Facebook's

computers.[5] We therefore hold that, after receiving written notification from Facebook on December 1, 2008, Power accessed Facebook's computers "without authorization" within the meaning of the CFAA and is liable under that statute.

Nosal I is materially distinguishable. First, *Nosal I* involved employees of a company who arguably exceeded the limits of their authorization. 676 F.3d at 856. Here, by contrast, Facebook explicitly revoked authorization for *any* access, and this case does not present the more nuanced question of exceeding authorization. *Nosal I* involved a defendant who "exceeded authorization," while this case involves a defendant who accessed a computer "without authorization." Second, although *Nosal I* makes clear that violation of the terms of use of a website cannot itself constitute access without authorization, this case does *not* involve non-compliance with terms and conditions of service. Facebook and Power had no direct relationship, and it does not appear that Power was subject to any contractual terms that it could have breached. Finally, *Nosal I* was most concerned with transforming "otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id.* at 860. It aimed to prevent criminal liability for computer users who might be

5. Simply bypassing an IP address, without more, would not constitute unauthorized use. Because a blocked user does not receive notice that he has been blocked, he may never realize that the block was imposed and that authorization was revoked. Or, even if he does discover the block, he could conclude that it was triggered by misconduct by someone else who shares the same IP address, such as the user's roommate or co-worker.

unaware that they were committing a crime. But, in this case, Facebook clearly notified Power of the revocation of access, and Power intentionally and admittedly refused to comply. *Nosal I*'s concerns about overreaching or an absence of culpable intent simply do not apply here, where an individualized cease-and-desist letter is a far cry from the permission skirmishes that ordinary Internet users may face.

Accordingly, we hold that, after receiving the cease and desist letter from Facebook, Power intentionally accessed Facebook's computers knowing that it was not authorized to do so, making Power liable under the CFAA. We therefore affirm in part the holding of the district court with respect to the CFAA.

C. Section 502

California Penal Code section 502 imposes liability on a person who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." *Id.* § 502(c)(2). This statute, we have held, is "different" than the CFAA. *United States v. Christensen*, 801 F.3d 970, 994 (2015). "[T]he California statute does not require *unauthorized* access. It merely requires *knowing* access." *Id.*

But despite differences in wording, the analysis under both statutes is similar in the present case. Because

Power had implied authorization to access Facebook's computers, it did not, at first, violate the statute. But when Facebook sent the cease and desist letter, Power, as it conceded, knew that it no longer had permission to access Facebook's computers at all. Power, therefore, knowingly accessed and without permission took, copied, and made use of Facebook's data. Accordingly, we affirm in part the district court's holding that Power violated section 502.

D. Personal Liability

We affirm the district court's holding that Vachani is personally liable for Power's actions. A "corporate officer or director is, in general, personally liable for all torts which he authorizes or directs or in which he participates, notwithstanding that he acted as an agent of the corporation and not on his own behalf." *Comm. for Idaho's High Desert, Inc. v. Yost*, 92 F.3d 814, 823 (9th Cir. 1996) (internal quotation marks omitted). Cases finding "personal liability on the part of corporate officers have typically involved instances where the defendant was the 'guiding spirit' behind the wrongful conduct, or the 'central figure' in the challenged corporate activity." *Davis v. Metro Prods., Inc.*, 885 F.2d 515, 523 n.10 (9th Cir. 1989) (internal quotation marks and ellipsis omitted).

Vachani was the central figure in Power's promotional scheme. First, Vachani admitted that, during the promotion, he controlled and directed Power's actions. Second, Vachani admitted that the promotion was his idea. It is undisputed, therefore, that Vachani was the guiding spirit and central figure in Power's challenged actions.

Accordingly, we affirm the district court's holding on Vachani's personal liability for Power's actions.

E. Discovery Sanctions

We affirm the discovery sanctions imposed against Power for non-compliance during a Rule 30(b)(6) deposition. Defendants failed to object to discovery sanctions in the district court. Failure to object forfeits Defendants' right to raise the issue on appeal. *Simpson v. Lear Astronics Corp.*, 77 F.3d 1170, 1174 (9th Cir. 1996).

Even assuming the issue was not waived, we "review the district court's rulings concerning discovery, including the imposition of discovery sanctions, for abuse of discretion." *Goodman v. Staples Office Superstore, LLC*, 644 F.3d 817, 822 (9th Cir. 2011). The magistrate judge's findings that Vachani was unprepared, unresponsive, and argumentative and that Power Ventures had failed to produce many e-mails responsive to Facebook's requests prior to discovery are supported by the record. Accordingly, we hold that the discovery sanctions imposed were not an abuse of discretion.

F. Remedies

Because we reverse in significant part, we also vacate the injunction and the award of damages. We remand the case to the district court to reconsider appropriate remedies under the CFAA and section 502, including any injunctive relief. With respect to damages, the district court shall calculate damages only for the period after

Power received the cease and desist letter, when Power continued to access data contained in Facebook's servers and memory banks.

REVERSED in part, **VACATED** in part, **AFFIRMED** in part, and **REMANDED**. The parties shall bear their own costs on appeal.

APPENDIX B — ORDER OF THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION, FILED FEBRUARY 16, 2012

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

NO. C 08-05780 JW

FACEBOOK, INC.,

Plaintiff,

v.

POWER VENTURES, INC., *et al*.,

Defendants.

Judges: JAMES WARE, Chief United States District Judge.

Opinion by: JAMES WARE

February 16, 2012, Decided
February 16, 2012, Filed

ORDER GRANTING PLAINTIFF'S MOTIONS FOR SUMMARY JUDGMENT; DENYING DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Appendix B

I. INTRODUCTION

Facebook, Inc. ("Plaintiff") brings this action against Defendants[1] alleging violations of the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"), 15 U.S.C. §§ 7701 *et seq.*, the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and California Penal Code § 502. Plaintiff alleges that Defendants accessed its website in an unauthorized manner, and then utilized this unauthorized access to send unsolicited and misleading commercial e-mails to Facebook users.

Presently before the Court are Plaintiff's Motions for Summary Judgment on Counts One,[2] Two and Three,[3] and Defendants' Motion for Summary Judgment on all counts.[4] The Court conducted a hearing on January 23, 2012. Based on the papers submitted to date and oral argument, the Court GRANTS Plaintiff's Motions for Summary

1. Defendants are Power Ventures, Inc. ("Power") and Steven Vachani ("Vachani").

2. (Facebook, Inc.'s Corrected Notice of Motion and Motion for Partial Summary Judgment on Count 1; Memorandum of Points and Authorities in Support Thereof, hereafter, "CAN-SPAM MSJ," Docket Item No. 215.)

3. (Notice of Motion, Motion and Memorandum of Points and Authorities for Partial Summary Judgment under California Penal Code § 502 and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, hereafter, "Fraud MSJ," Docket Item No. 214.)

4. (Notice of Motion, Motion, and Memorandum of Law in Support of Defendants' Motion for Summary Judgment, hereafter, "Defendants' MSJ," Docket Item No. 98.)

Judgment on all counts, and DENIES Defendants' Motion for Summary Judgment.

II. BACKGROUND

A. Undisputed Facts

Plaintiff owns and operates the widely popular social networking website located at http://www.facebook.com.[5] Defendant Power is a corporation incorporated in the Cayman Islands doing business in the State of California.[6] Defendants operate a website, www.power.com, which offers to integrate multiple social networking accounts into a single experience on Power.com. (FAC ¶ 5; Answer ¶ 5.) Defendant Vachani is the CEO of Power. (*Id.* ¶ 11; *Id.* ¶ 11.)

Users of Plaintiff's website register with a unique username and password. (FAC ¶ 21; Answer ¶ 21.) Before Plaintiff activates a username and permits a user to access certain features of Facebook, the user must agree to Plaintiff's Terms of Use. (*Id.* ¶ 29; *Id.* ¶ 29.) The Terms of Use require users to refrain from using automated scripts to collect information from or otherwise interact with Facebook, impersonating any person or entity, or using Facebook website for commercial use without the express permission of Facebook. (*Id.* ¶ 30; *Id.* ¶ 30.)

---

5. (First Amended Complaint ¶ 20, hereafter, "FAC," Docket Item No. 9; Amended Answer and Counterclaims of Defendants Power Ventures, Inc. and Steve Vachani ¶ 20, hereafter, "Answer," Docket Item No. 54.)

6. (FAC ¶ 10; Answer ¶ 10.)

Appendix B

On or before December 1, 2008, Power began advertising and offering integration with Plaintiff's site. (FAC ¶ 49; Answer ¶ 49.) Power permitted users to enter their Facebook account information and access Facebook site through Power.com. (*Id.* ¶ 50; *Id.* ¶ 50.) At no time did Defendants receive permission from Plaintiff to represent that solicitation of Facebook usernames and passwords was authorized or endorsed by Plaintiff. (*Id.* ¶ 53; *Id.* ¶ 53.)

On or before December 26, 2008, Power began a "Launch Promotion" that promised Power.com's users the chance to win one hundred dollars if they successfully invited and signed up new Power.com users. (FAC ¶ 65; Answer ¶ 65.) As part of this promotion, Power provided participants with a list of their Facebook friends, obtained by Power from Facebook, and asked the participant to select which of those friends should receive a Power invitation. (*Id.* ¶ 66; *Id.* ¶ 66.) The invitations sent to those friends purport to come from "Facebook" and used an "@facebookmail.com" address, not a Power.com address. (*Id.* ¶ 68; *Id.* ¶ 68.)

On December 1, 2008, Plaintiff notified Defendant Vachani of its belief that Power's access of Plaintiff's website and servers was unauthorized and violated Plaintiff's rights. (FAC ¶ 57; Answer ¶ 57.) Facebook subsequently implemented technical measures to block users from accessing Facebook through Power.com. (*Id.* ¶ 63; *Id.* ¶ 63.)

B. Procedural History

On December 30, 2008, Plaintiff filed its initial Complaint. (*See* Docket Item No. 1.) On January 13, 2009,

Plaintiff filed the First Amended Complaint naming both Power Ventures and Vachani as Defendants. (*See* FAC at 1.) On March 23, 2009, Defendants moved to dismiss Plaintiff's Complaint or, in the alternative, for a more definite statement. (*See* Docket Item No. 17.) On May 11, 2009, the Court denied Defendants' Motion to Dismiss as to all claims. (*See* Docket Item No. 38.) On November 23, 2009, Defendants answered Plaintiff's First Amended Complaint and asserted counterclaims under the Sherman Antitrust Act and California's Unfair Competition Law. (*See* Answer ¶¶ 167-185.)

On December 23, 2009, Plaintiff filed a Motion for Judgment on the Pleadings or, in the Alternative, Partial Summary Judgment of Liability Under California Penal Code Section 502(c). (*See* Docket Item No. 56.) The same day, Plaintiff also filed a Motion to Dismiss Defendants' Counterclaims and Strike Defendants' Affirmative Defenses. (*See* Docket Item No. 58.) On January 15, 2010, Defendants filed a Cross-Motion for Summary Judgment. (*See* Docket Item No. 62.) On February 26, 2010, Judge Fogel recused himself from the case. (*See* Docket Item No. 72.) On March 2, 2010, the case was reassigned to Judge Ware. (*See* Docket Item No. 73.) On July 20, 2010, the Court denied Plaintiff's Motion for Judgment on the Pleadings or Summary Judgment, denied Plaintiff's Motion to Strike Defendants' Affirmative Defenses, denied Defendants' Motion for Summary Judgment and granted Plaintiff's Motion to Dismiss Defendants' Counterclaims.[7]

---

7. (*See* Order Denying Facebook's Motion for Judgment on the Pleadings; Denying the Parties' Cross-Motions for Summary Judgment; Granting Facebook's Motion to Dismiss Defendants' Counterclaims; Denying Facebook's Motion to Strike Defendants'

Appendix B

Presently before the Court are the parties' Motions for Summary Judgment.

III. STANDARDS

Summary judgment is proper when the moving party shows that there is no genuine dispute as to any material fact. Fed. R. Civ. P. 56(a). The purpose of summary judgment "is to isolate and dispose of factually unsupported claims or defenses." *Celotex v. Catrett*, 477 U.S. 317, 323-24, 106 S. Ct. 2548, 91 L. Ed. 2d 265 (1986). The moving party "always bears the initial responsibility of informing the district court of the basis for its motion, and identifying the evidence which it believes demonstrates the absence of a genuine issue of material fact." *Id.* at 323. If the moving party meets its initial burden, the "burden then shifts to the nonmoving party to establish, beyond the pleadings, that there is a genuine issue for trial." *Miller v. Glenn Miller Prods., Inc.*, 454 F.3d 975, 987 (9th Cir. 2006) (citing *Celotex*, 477 U.S. at 324).

When evaluating a motion for summary judgment, the court views the evidence through the prism of the evidentiary standard of proof that would pertain at trial. *Anderson v. Liberty Lobby Inc.*, 477 U.S. 242, 255, 106 S. Ct. 2505, 91 L. Ed. 2d 202 (1986). The court draws all reasonable inferences in favor of the non-moving party, including questions of credibility and of the weight that particular evidence is accorded. *See, e.g., Masson v. New*

Affirmative Defenses, hereafter, "July 20 Order," Docket Item No. 89.)

Yorker Magazine, Inc., 501 U.S. 496, 520, 111 S. Ct. 2419, 115 L. Ed. 2d 447 (1992). The court determines whether the non-moving party's "specific facts," coupled with disputed background or contextual facts, are such that a reasonable jury might return a verdict for the non-moving party.

T.W. Elec. Serv. v. Pac. Elec. Contractors, 809 F.2d 626, 631 (9th Cir. 1987). In such a case, summary judgment is inappropriate. *Anderson*, 477 U.S. at 248. However, where a rational trier of fact could not find for the non-moving party based on the record as a whole, there is no "genuine issue for trial." *Matsushita Elec. Indus. Co. v. Zenith Radio*, 475 U.S. 574, 587, 106 S. Ct. 1348, 89 L. Ed. 2d 538 (1986).

Although the district court has discretion to consider materials in the court file not referenced in the opposing papers, it need not do so. *See Carmen v. San Francisco Unified Sch. Dist.*, 237 F.3d 1026, 1028-29 (9th Cir. 2001). "The district court need not examine the entire file for evidence establishing a genuine issue of fact." *Id.* at 1031. However, when the parties file cross-motions for summary judgment, the district court must consider all of the evidence submitted in support of both motions to evaluate whether a genuine issue of material fact exists precluding summary judgment for either party. *Fair Housing Council of Riverside Cnty, Inc. v. Riverside Two*, 249 F.3d 1132, 1135 (9th Cir. 2001).

Appendix B

IV. DISCUSSION

Plaintiff moves for summary judgment on the grounds that: (1) the undisputed evidence establishes that Defendants sent misleading commercial e-mails through Facebook's network in violation of the CAN-SPAM Act;[8] and (2) the undisputed evidence also establishes that Defendants utilized technical measures to access Facebook without authorization, in violation of both the CFAA and California Penal Code Section 502.[9] Defendants respond that: (1) because Plaintiff's own servers sent the commercial e-mails at issue, Defendants did not initiate the e-mails as a matter of law; and (2) Defendants did not circumvent any technical barriers in order to access Facebook site, precluding liability under the CFAA or Section 502.[10] Defendants further contend that Plaintiff suffered no damages as a result of Defendants' actions, and thus lacks standing to bring a private suit for Defendants' conduct. (*Id.* at 15-16, 19-20.)

A. The CAN-SPAM Act

At issue is whether the conduct of Defendants, as established by the undisputed evidence, constitutes a violation of the CAN-SPAM Act.

The CAN-SPAM Act provides that "[i]t is unlawful

---

8. (CAN-SPAM MSJ at 12-16.)

9. (Fraud MSJ at 1.)

10. (Defendants' MSJ at 5, 16-17.)

for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). The Act also creates a private right of action for internet service providers adversely affected by violations of this provision. *See id.* § 7706(g)(1). To prevail on a CAN-SPAM Act claim, a plaintiff must establish not only that the defendant violated the substantive provisions of the Act, but also that the plaintiff was adversely affected by this violation such that it satisfies the statutory standing requirements. *See Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1048 (9th Cir. 2009). The Court considers each requirement in turn.

1. Standing

At issue is whether Plaintiff has standing to assert a claim under the CAN-SPAM Act.

Standing under Section 7706 "involves two general components: (1) whether the plaintiff is an 'Internet access service' provider ('IAS provider'), and (2) whether the plaintiff was 'adversely affected by' statutory violations." *Gordon*, 575 F.3d at 1049 (citation omitted).

Here, Defendants concede that Plaintiff is an IAS provider.[11] Therefore, the only question before the Court in determining Plaintiff's standing is whether Plaintiff was "adversely affected" by the alleged violations at issue.

11. (*See* Defendants' MSJ at 13.)

Appendix B

In *Gordon*, the Ninth Circuit explained that not all possible harms to an IAS provider constitute harm within the meaning of the Act, and distinguished those harms sufficient to confer standing from those outside the scope of Congress' intent. *See* 575 F.3d at 1049-55. After discussing the congressional decision to confer standing upon IAS providers but not end-consumers affected by commercial e-mails, the court concluded that "[l]ogically, the harms redressable under the CAN-SPAM Act must parallel the limited private right of action and therefore should reflect those types of harms uniquely encountered by IAS providers." *Id.* at 1053. Thus, while the "mere annoyance"[12] of spam encountered by all e-mail users is not sufficient to confer standing, the court identified the costs of investing in new equipment to increase capacity, customer service personnel to address increased subscriber complaints, increased bandwidth, network crashes, and the maintenance of anti-spam and filtering technologies as the "sorts of ISP-type harms" that Congress intended to confer standing. *Id.* at 1053. Thus, the court noted, "[i]n most cases, evidence of some combination of operational or technical impairments and related financial costs attributable to unwanted commercial e-mail would suffice." *Id.* at 1054 (citation omitted).

Here, in support of its contention that it has standing to pursue a CAN-SPAM Act claim, Plaintiff offers the following evidence:

---

12. *Id.* at 1053-54.

Appendix B

(1) Around December 1, 2008 Ryan McGeehan, manager of Plaintiff's Security Incident Response Team ("SIR Team"), determined that Power was running an automated scripting routine to harvest data and download it to the Power.com website.[13] McGeehan then spent substantial time and effort determining what steps were necessary to contain Power's spamming. (*Id.* ¶ 12.) It was determined that at least 60,627 event invitations were sent to Facebook users due to Power's activities. (*Id.*) On December 12, 2008, after Plaintiff's counsel sent Power a cease and desist letter, and the activity did not stop, Plaintiff attempted to block Power's access by blocking what appeared to be its primary IP address. (*Id.* ¶ 13.) On December 22, 2008, McGeehan determined that Power was still accessing Facebook through new IP addresses. (*Id.* ¶ 14.) Plaintiff then attempted to block these IP addresses as well. (*Id.* ¶ 13.) In early 2009, Facebook blacklisted the term Power.com, preventing that term from appearing anywhere on the site. (*Id.* ¶ 16.) In implementing these measures, McGeehan spent at least three to four days of his own

13. (*See* Declaration of Ryan McGeehan in Support of Facebook's Motion for Partial Summary Judgment on Count 1 Under the CAN-SPAM Act ¶¶ 1, 7, hereafter, "McGeehan Decl.," Docket Item No. 213-4.)

engineering time addressing security issues presented by Power. (*Id.* ¶ 17.)

(2) On December 1, 2008, Joseph Cutler sent a cease and desist letter to Power.com.[14] After this letter was sent Cutler was contacted by Steve Vachani, who identified himself as the owner and operator of Power Ventures. (*Id.* ¶ 7.) In this and subsequent discussions, Vachani assured Cutler that the functionality of the Power website would be changed to comply with Facebook's requests. (*Id.* ¶¶ 9-10.) On December 27, 2008, Cutler received an e-mail saying that Power Ventures would not change its website as earlier stated. (*Id.* ¶ 13.) From fall of 2008 through early 2009, Facebook spent approximately $75,000 on Cutler's firm related to Power Venture's actions. (*Id.* ¶ 15.)

Defendants do not dispute the accuracy or veracity of this evidence of Plaintiff's expenditures. Instead, Defendants contend that, as a matter of law, these are not the sorts of harm that give rise to standing under *Gordon*, as they fall within the category of negligible

14. (*See* Declaration of Joseph Cutler in Support of Facebook, Inc.'s Motion for Partial Summary Judgment for Liability Under the CAN-SPAM Act ¶ 6, hereafter, "Cutler Decl.," Docket Item No. 213-2.)

burdens routinely borne by IAS providers.[15] In support of this contention, Defendants rely on the following evidence:

(1) In the fourth quarter of 2008, Plaintiff received 71,256 user complaints that contained the word "spam." (McGeehan Decl. ¶ 5.) Facebook did not produce any evidence of customer complaints specifically referencing the e-mails at issue in this case.[16]

(2) Craig Clark, litigation counsel at Facebook, testified that he was not aware of any documents that would be responsive to any of the requests for production made by Defendants.[17] These requests for production

---

15. (Defendants' Memorandum of Points and Authorities in Opposition to Facebook's Motion for Partial Summary Judgment on Count 1 (CAN-SPAM Act, 15 U.S.C. § 7704) at 14-15, hereafter, "CAN-SPAM Opp'n," Docket Item No. 234.)

16. (*See* Declaration of L. Timothy Fisher in Support of Defendants' Motion for Summary Judgment ¶ 4, hereafter, "Fisher Decl.," Docket Item No. 106; *see also* Fisher Decl., Ex. B, Facebook, Inc.'s Objections and Response to Defendants' Requests for Production, Set One, Docket Item No. 106.)

17. (Fisher Decl., Ex. C, Deposition of Craig Clark at 118:20-118:23, hereafter, "Clark Depo.," Docket Item No. 106.) Plaintiff objects to Defendants' reliance on Mr. Clark's testimony because Mr. Clark was deposed in his personal capacity, rather than pursuant to Fed. R. Civ. P. 30(b)(6), and thus Plaintiff contends that Mr. Clark's answers to the questions presented to him are irrelevant because he does not speak on behalf of Facebook. (*See* Docket Item No. 240

> included requests for all documents regarding any injury that Plaintiff suffered, expenditures Plaintiff made, or user complaints that Plaintiff received as a result of the events complained of in Plaintiff's First Amended Complaint.[18]

Upon review, on the basis of these undisputed facts, the Court finds that Plaintiff has demonstrated an "adverse effect" from Defendants' conduct sufficient to confer standing. The evidence submitted by Plaintiff is not limited to documenting a general response to spam prevention, but rather shows acts taken and expenditures made in response to Defendants' specific acts.[19] These specific responses to Defendants' actions distinguish Plaintiff's damages from those in the cases relied upon by Defendants, which asserted only the costs of general spam prevention as the basis for standing.[20] In particular, since Plaintiff documented a minimum of 60,000 instances of spamming by Defendants, the costs of responding to

---

at 17-23.) For the purposes of this Order only, Plaintiff's objection to the Clark deposition is OVERRULED because harm to Plaintiff is established irregardless of Mr. Clark's testimony.

18. (Fisher Decl., Ex. A, Defendants' First Requests for Production Pursuant to Fed. R. Civ. P. 34, Docket Item No. 106.)

19. (*See, e.g.*, McGeehan Decl. ¶¶ 8-17; *see also id.*, Ex. 4, Electronic Ticket Documenting McGeehan's Attempts to Block Defendant's Access to Facebook, Docket Item No. 213-7.)

20. (*See, e.g.*, CAN-SPAM Opp'n at 15 (citing *ASIS Internet Servs. v. Azoogle.com, Inc.*, 357 Fed. Appx. 112, 113-14 (9th Cir. 2009).)

such a volume of spamming cannot be categorized as "negligible." *See Gordon*, 575 F.3d at 1055-56. The Court finds that under *Gordon* and *Azoogle*, though the general costs of spam prevention may not confer standing under the CAN-SPAM Act, documented expenditures related to blocking a specific offender may. This is particularly true where, as here, Defendants' spamming activity was ongoing, prolific, and did not stop after requests from the network owner. Thus, as the undisputed evidence establishes that Plaintiff expended significant resources to block Defendants' specific spamming activity, the Court finds that Plaintiff has standing to maintain a CAN-SPAM action.

2. Merits of CAN-SPAM Act Claim

At issue is whether Defendants' conduct, as established by the undisputed facts, violates the substantive provisions of the CAN-SPAM Act. The Act makes it unlawful, *inter alia*, "for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Defendants contend that Plaintiff's CAN-SPAM Act claim must fail because: (1) the undisputed facts establish that Plaintiff itself, and not Defendants, initiated the e-mails at issue; and (2) because Plaintiff sent the e-mails, the header information identifying Facebook as the sender was accurate and not misleading.[21] The Court considers each element in turn.

21. (Defendants' MSJ at 12-14.)

Appendix B

a. Initiation of Commercial E-mails

At issue is whether Defendants initiated the e-mails associated with the Launch Promotion.

The CAN-SPAM Act provides that "[t]he term 'initiate,' when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message." 15 U.S.C. § 7702(9). The word "procure," in turn, is defined to mean "intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one's behalf." *Id.* § 7702(12).

In support of its claim that Defendants initiated the e-mails at issue, Plaintiff offers the following undisputed evidence:

(1) On or before December 26, 2008, Defendant Power began a "Launch Promotion" that offered site users $100 if they successfully invited and signed up the most new Power.com users. (FAC ¶ 65; Answer ¶ 65.) As part of the promotion, Power obtained a list of the user's Facebook friends and asked the participant to select which of those friends should receive a Power.com invitation. (*Id.* ¶ 66; *Id.* ¶ 66). Selected friends would then

receive an e-mail in which Facebook was listed as the sender, promoting an event "Bring 100 Friends and win 100 bucks!" (*Id.* ¶70; *Id.* ¶ 70.) Defendant admits that Power.com's "offer of potential monetary compensation may have induced some Facebook users to participate in Power's launch program." (*Id.* ¶ 72; *Id.* ¶ 72.)

(2) The testimony of Vachani that Power.com both authored the text contained in the e-mails and provided the link contained therein that would allow recipients to sign up for Power.com.[22]

(3) The launch promotion feature that offered the $100 reward was made available to Power.com users through Power.com. (Vachani Depo. at 264:2-264:8.) None of the social networking networks on Power.com created the contents of the launch promotion feature. (*Id.* at 264:9-264:12.)

(4) The declaration of Facebook's technical expert, Lawrence Melling, that based on his study of the software created by Defendant Power and its code, the script

22. (Declaration of Monte M.F. Cooper in Support of Facebook, Inc.'s Motion for Partial Summary Judgment on Count 1 under the CAN-SPAM Act, hereafter, "Cooper Decl.," Ex. 2, Deposition of Steven Vachani at 197:4-197:12, hereafter, "Vachani Depo.," Docket Item No. 229.)

would automatically insert Power as the host of the event and the event location. [23] The script also automatically generated a guest list for the event if one was not provided, and did so by accessing the user's Facebook friends list. (*Id.* ¶ 19.) The script would then automatically send Facebook event invitations to each Facebook user on the guest list on behalf of Power. (*Id.* ¶ 20.)

(5) The testimony of Vachani that Power eventually paid 30-40 people who got 100 or more friends to sign up. (Vachani Depo. at 189:5-9.)

Defendants, while not disputing the accuracy of the above facts, contend that as a matter of law, they did not "initiate" the e-mails at issue because the e-mails were authorized by Facebook users and sent from Facebook's own servers.[24] In support of this contention, Defendants rely upon the facts, also undisputed, that after a user authorized the creation of an event as part of the Launch Promotion, Facebook servers automatically filled in the header information and sent an e-mail to each person on the event guest list.[25]

---

23. (Declaration of Lawrence Melling in Support of Facebook, Inc.'s Motion for Partial Summary Judgment on Count 1 of the CAN-SPAM Act ¶ 18, hereafter, "Melling Decl.," Docket Item No. 217.)

24. (*See* Defendants' MSJ at 5-8.)

25. (*See* Clark Depo. at 98:18-99:25.)

Upon review, the Court finds that based on these undisputed facts, Defendants initiated the emails sent through the Launch Promotion. Although Facebook servers did automatically send the emails at the instruction of the Launch Program, it is clear that Defendants' actions-in creating the Launch Promotion, importing users' friends to the guest list, and authoring the e-mail text-served to "originate" the e-mails as is required by the Act.[26] To hold that Plaintiff originated the e-mails merely because Facebook servers sent them would ignore the fact that Defendants intentionally caused Facebook's servers to do so, and created a software program specifically designed to achieve that effect. Further, while Defendants emphasize that Facebook users authorized the creation of events resulting in the e-mails,[27] the Court finds that Defendants procured these users to do so by offering and awarding monetary incentives to provide such authorization. Thus, even if Facebook users may be viewed as initiators of the e-mails because of their participation in the Launch Promotion, Defendants are nonetheless also initiators as a matter of law because of their procurement of user participation.[28]

Accordingly, the Court finds that Defendants did initiate the e-mails at issue within the meaning of the CAN-SPAM Act.

---

26. *See* 15 U.S.C. § 7702(9).

27. (*See, e.g.*, Defendants' MSJ at 7.)

28. *See* 15 U.S.C. § 7702(12).

b. Whether the E-mails Are Misleading

At issue is whether the e-mails sent as a result of the Launch Promotion contain header information that is false or misleading.

The CAN-SPAM Act defines header information as "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." 15 U.S.C. § 7702(8). The Act further provides that "header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin." *Id.* § 7704(a)(1)(C). A false or misleading statement is considered material if "the alteration or concealment of header information" would impair the ability of an IAS provider or a recipient to "identify, locate, or respond to a person who initiated the electronic mail message." *Id.* § 7704(a)(6).

Here, for the reasons discussed above, Defendants were initiators of the e-mail messages at issue. But because Defendants' program caused Facebook servers to automatically send the e-mails, these e-mails contained an "@facebookmail.com" address.[29] These e-mails did not contain any return address, or any address anywhere in the e-mail, that would allow a recipient to respond to

29. (FAC ¶¶ 68-69; Answer ¶¶ 68-69.)

Defendants.[30] Thus, as the header information does not accurately identify the party that actually initiated the e-mail within the meaning of the Act, the Court finds that the header information is materially misleading as to who initiated the e-mail.

Defendants contend that even if the Court finds that they did initiate the e-mails at issue, they cannot be held liable for violations of the CAN-SPAM Act on the grounds that: (1) the text of the emails itself includes information about Power.com; and (2) Defendants had no control over the headers of the e-mails.[31] The Court finds that both of these contentions are unavailing. First, the presence of a misleading header in an e-mail is, in and of itself, a violation of the CAN-SPAM Act, insofar as the Act prohibits the use of misleading header information.[32] Thus, the fact that the text of the e-mails at issue may have

---

30. (Declaration of Theresa Sutton in Support of Plaintiff Facebook, Inc.'s Opposition to Defendants' Motion for Summary Judgment, hereafter, "Sutton Decl.," Ex. 4, Defendant Power Ventures, Inc.'s Responses to Facebook, Inc.'s First Set of Requests for Admissions at No. 50, hereafter, "Defendants' Admissions," Docket Item No. 241-3.)

31. (Defendant's Motion at 14.) The latter argument was also made by *Amicus Curiae* Electronic Frontier Foundation ("EFF"), which contends that because the Facebook system auto-generates the header information provided in the e-mails, commercial users should not be held responsible for their content. (*See* Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant Power Ventures' Motion for Summary Judgment on Count 1 (CAN-SPAM Act, 15 U.S.C. § 7704) and Under California Penal Code § 502 and the Computer Fraud and Abuse Act at 18-19, hereafter, "EFF Brief," Docket Item No. 206-2.)

32. *See* 15 U.S.C. § 7704(a)(1).

included information about Power.com is irrelevant, for purposes of liability under the Act. Second, the question of whether Defendants had control over the headers is also irrelevant. In particular, the Court finds that the fact that Defendants used a program that was created and controlled by another to send e-mails with misleading headers does not absolve them of liability for sending those e-mails.[33]

In sum, the Court finds that the undisputed facts establish that Defendants initiated the sending of e-mails with false or misleading heading information under the CAN-SPAM Act, and that Plaintiff suffered adverse effects as contemplated by the Act sufficient to convey standing to maintain a private cause of action. Accordingly, the Court GRANTS Plaintiff's Motion for Summary Judgment on Count One, and DENIES Defendants' Motion for Summary Judgment as to Count One.

---

33. Amicus EFF contends that the CAN-SPAM Act's prohibition on the sending of misleading commercial e-mails should not be applied to e-mails sent through a system like that of Facebook, in which the headers are auto-generated by servers and not controlled by the individual users. (EFF Brief at 20.) However, the Court finds no statutory basis for creating such an exception to the CAN-SPAM Act. The Act makes it unlawful to "initiate the transmission" of any e-mail message that is "accompanied by" misleading header information. 15 U.S.C. § 7704(a)(1). Nothing in this language requires that the user actually create the misleading header information, as opposed to utilizing a system already in place to auto-generate a header.

Appendix B

B. California Penal Code § 502

At issue is whether Defendants' conduct, as established by the undisputed facts, violated California Penal Code § 502 ("Section 502").

Section 502(c) provides that a person is guilty of a public offense if he, *inter alia*: (1) knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network; (2) knowingly and without permission uses or causes to be used computer services; or (3) knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. *See* Cal. Penal Code § 502(c)(2), (3) & (7). Section 502(e) provides that "the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief." *See id.* § 502(e).

Here, the Court has already held that Plaintiff has suffered sufficient harm to have standing under Section 502. (*See* July 20 Order at 8.) In addition, Defendants admit that they took, copied, or made use of data from Facebook website without Facebook's permission to do so. (Defendants' Admissions at 22.) Therefore the only question remaining before the Court, in determining whether Defendants violated Section 502, is whether

Defendants' access to Facebook was "without permission" within the meaning of Section 502.[34]

In its July 20 Order, the Court explained at great length that a particular use of a computer network which violates that network's terms of use is insufficient to establish that the use was "without permission" pursuant Section 502.[35] Where, however, a party accesses the network in a manner that circumvents technical or code-based barriers in place to restrict or bar a user's access, then the access does qualify as being "without permission." (*See id.* at 18-20.) Accordingly, the question before the Court is whether the undisputed evidence establishes that Defendants circumvented technical or code-based barriers in order to access Facebook.

In support of the contention that Defendants did circumvent technical barriers designed to block their access to Facebook, Plaintiff relies on the following evidence:

---

34. Defendants continue to contend that Plaintiff did not suffer any loss as is required by Section 502 and therefore lacks standing to bring a private cause of action. (*See* Defendants' MSJ at 19-20.) In so doing, Defendants suggest that the Court's July 20 Order declined to reach the issue of loss because it denied both parties' motions for summary judgment at that time. (*Id.*) The Court finds, however, that this interpretation of its Order is misguided, as it ignores the plain statement that "[s]ince the undisputed facts demonstrate that Facebook has suffered some damage or loss in attempting to block Power's access to Plaintiff's website, the Court finds that Facebook has standing to bring suit under Section 502." (July 20 Order at 8.)

35. (*See* July 20 Order at 8-20.)

(1) In response to the question if he at any time became aware that Facebook was attempting to block Power, Vachani answered: "I don't know if they were—[o]bviously, we expected that they would but he we [sic] also know that our system doesn't get blocked because there's nothing—there's nothing it's technically doing. It's just users accessing the site so that it can't really be blocked . . . .We know [sic] that they would try, but we also know that it was built to — it would not be blockable."[36]

(2) The expert of report of Bob Zeidman and Lawrence Melling, who analyzed the code and software used by Power.com to determine if it was designed to circumvent technical barriers.[37] The report concludes that the code used a number of routines to avoid being blocked by websites like Facebook, including the use of proxy servers if one server was blocked by a website. (*Id.*

---

36. (Declaration of Morvarid Metanat in Support of Facebook's Motion for Partial Summary Judgment Under California Penal Code § 502 and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, hereafter, "Metanat Decl.," Ex. 2, Deposition of Steve Vachani at 323:17-324:8, hereafter, "Vachani Depo. 2," Docket Item No. 236-2.)

37. (Expert Report of Bob Zeidman and Lawrence Melling ¶¶ 25, filed under seal.) This Report was filed under seal. However, the Court finds that the portions of the Report discussed in this Order were not appropriately sealed. Accordingly, the Court UNSEALS the Report for purposes of discussing its contents in this Order.

¶¶ 55-60.) The code would routinely monitor each server to see if an IP address was blocked and change the IP address if it was. (*Id.* ¶¶ 59-60.) The report concludes that substantial effort went into designing the proxy system and that one of the objectives of the design was to reconfigure the IP connections if an IP address was blocked. (*Id.* ¶ 61.)

(3) The testimony of Ryan McGeehan that on December 12, 2008, Facebook attempted to block Power's access to the site by blocking what appeared to be its primary IP address. (McGeehan Decl. ¶ 13.) Following the block, Facebook determined that Powers was circumventing the block by using other IP addresses. (*Id.*) Facebook attempted to block these addresses as they discovered them "in a game of cat and mouse." (*Id.*)

(4) An e-mail from Vachani to members of his staff, sent after Vachani received a cease and desist letter from Plaintiff, stating "we need to be prepared for Facebook to try and block us and then turn this into a national battle that gets us huge attention."[38]

(5) A transcript of a discussion between Vachani and a member of his staff in which

38. (Metanat Decl., Ex. 6, E-mail from Steven Vachani, Docket Item No. 236-6; *see also* Vachani Depo. 2 at 313:3-313:7.)

> the they discuss the process of starting to fetch profile data from another social networking website, Orkut.[39] Vachani says "we also need to do some planning to make sure that we do it in a way where we are not really detected. [P]ossible rotating IP's or something. [D]on't really understand this too well. Greg may also have some ideas." (*Id.* at 3.) The staff member responds "yah. [R]otating IP if we can set then its very good as when [O]rkut will see so much band[w]idth use by perticular [sic] IP then they will block that perticulat [sic] IP." (*Id.* at 3-4.) Vachani responds "We need to plan this very carefully since we will have only one chance to do it. . . we might need to rotate with over 200 IP's or even more to do it perfectly." (*Id.* at 4.)

In support of their contention that they did not circumvent technical barriers imposed by Plaintiff, Defendants offer the following evidence:

> Vachani's testimony that in December 2008, Facebook attempted to prevent Power's users from accessing Facebook through Power.com

---

39. (Declaration of I. Neel Chatterjee in Support of Reply Memorandum in Support of Facebook's Motions for Partial Summary Judgment Under: 1) on [sic] Count 1 the Can-Spam Act; and 2) California Penal Code § 502 and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, Ex. 2, Docket Item No. 248-2.)

> by blocking one IP address utilized by Power.[40] "Facebook's IP block was ineffective because it blocked only one outdated IP address Power had used, and did not block other IPs that Power was using in the normal course of business." (*Id.* ¶ 11.) "Power did not undertake any effort to circumvent that block, and did not provide users with any tools designed to circumvent it." (*Id.*) After it became aware of the attempted IP blocking, Power undertook efforts to implement Facebook Connect as Facebook had requested. (*Id.* ¶ 12.)[41]

Upon review, the Court finds that the undisputed facts establish that Defendants circumvented technical barriers to access Facebook site, and thus accessed the site "without permission." Although the evidence shows that Defendants did not take additional steps to circumvent individual IP blocks imposed by Plaintiff after the fact,

---

40. (Declaration of Steve Vachani in Support of Defendants' Opposition to Facebook's Motions for Partial Summary Judgment on Count 1 (Can-spam Act, 15 U.S.C [sic] § 7704) and Under California Penal Code § 502 and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ¶ 10, Docket No. 189.)

41. Plaintiff objects to Vachani's testimony regarding Facebook's blocks of the Power site on the grounds that Vachani lacks personal knowledge of how such technical measures worked and because he is not an expert qualified to opine on the functionality of a technical barrier. (*See* Docket Item No. 240 at 14.) For purposes of this Order only, the Court finds that Vachani's lack of qualifications as an expert affects the weight his testimony should be accorded and not its admissibility. Thus, Plaintiff's objection is OVERRULED.

this does nothing to cast doubt on the overwhelming evidence that Defendants designed their system to render such blocks ineffective. The Court finds no reason to distinguish between methods of circumvention built into a software system to render barriers ineffective and those which respond to barriers after they have been imposed. This is particularly true where, as here, Defendant Vachani's own statements provide compelling evidence that he anticipated attempts to block access by network owners and intentionally implemented a system that would be immune to such technical barriers.[42] Thus, in light of the undisputed evidence that Defendants anticipated attempts to block their access by Plaintiff, and utilized multiple IP addresses to effectively circumvent these barriers, the Court finds that Defendants violated Section 502 by accessing Plaintiff's network without permission.

Accordingly, the Court GRANTS Plaintiff's Motion for Summary Judgment as to Count Three and DENIES Defendants' Motion for Summary Judgment as to Count Three.

C. The Computer Fraud and Abuse Act

At issue is whether Defendants' conduct constitutes a violation of the CFAA.

The CFAA imposes liability on any party that "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains,"

42. (*See, e.g.*, Vachani Depo. 2 at 323:17-324:8.)

inter alia, "information from any protected computer." 18 U.S.C. § 1030(a)(2). Suit may be brought by any person who suffers damage or loss in an amount above $5000. *See id.* §1030(g); §1030(c)(4)(A)(i)(I).

Here, for the reasons discussed above, the undisputed facts establish that Defendants' access to Facebook was without authorization. In addition, Defendants admit that they obtained information from Facebook website. (Defendants' Admissions at 22.) Thus, the only finding necessary for Plaintiff to prevail on its CFAA claim is whether Plaintiff's damages exceed $5000, thereby giving Plaintiff standing under the statute.[43]

The CFAA defines "loss" to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). "Costs associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute." *Multiven*, 725 F. Supp. 2d at 895 (citation omitted).

Here, as discussed above with regard to Plaintiff's CAN-SPAM claim, Plaintiff has provided uncontradicted evidence of the costs of attempting to thwart Defendants'

43. *See Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010) (explaining that elements of a CFAA claim do not differ materially from the elements of a claim under Section 502).

unauthorized access into its network.[44] These documented costs were well in excess of the $5000 CFAA threshold. (*See* Cutler Decl. ¶ 15.) Thus, the Court finds that on the basis of these costs, Defendants' unauthorized access of Plaintiff's network did cause sufficient loss to Plaintiff to confer standing upon Plaintiff.

In sum, for the reasons discussed above regarding Plaintiff's Section 502 claim, the Court finds that Defendants accessed Plaintiff's website without authorization and obtained information from Facebook. The Court further finds that Plaintiff suffered loss sufficient to confer standing as a result of such access. Accordingly, the Court GRANTS Plaintiff's Motion for Summary Judgment as to Count Two and DENIES Defendants' Motion for Summary Judgment as to Count Two.

V. CONCLUSION

The Court GRANTS Plaintiff's Motions for Summary Judgment on all counts. The Court DENIES Defendants' Motion for Summary Judgment on all counts.[45]

---

44. (*See, e.g.*, McGeehan Decl. ¶¶ 11-17; Cutler Decl. ¶¶ 7-15.)

45. Because the Court finds that the undisputed evidence submitted by Plaintiff with its Motions for Summary Judgment establishes that Plaintiff is entitled to judgment as a matter of law, the Court DENIES as moot Plaintiff's Motion to File Supplemental Evidence. (*See* Docket Item No. 251.)

In addition, the Court DENIES as moot Plaintiff's Motion to Enlarge Time for Hearing Dispositive Motions. (*See* Docket Item No. 261.)

Appendix B

In light of this Order, the Court finds that additional briefing is warranted on two issues: (1) the amount of damages Plaintiff should receive in light of this Order; and (2) the individual liability of Defendant Vachani.

On or before **March 2, 2012**, the parties shall file simultaneous briefings addressing the two issues identified above. Unless otherwise indicated by the Court, the matter will be taken under submission for decision without a hearing. *See* Civ. L.R. 7-1(b).

Dated: February 16, 2012

/s/ James Ware
JAMES WARE
United States District Chief Judge

APPENDIX C — ORDER OF THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION, FILED SEPTEMBER 25, 2013

UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

Case No.: 08-CV-5780-LHK

FACEBOOK, INC.,

Plaintiff,

v.

POWER VENTURES, INC., A CAYMAN ISLAND CORPORATION, AND STEVE VACHANI, AN INDIVIDUAL,

Defendants.

September 25, 2013, Decided;
September 25, 2013, Filed

ORDER DENYING LEAVE TO FILE MOTION FOR RECONSIDERATION, FINDING DEFENDANT STEVEN VACHANI LIABLE AS A MATTER OF LAW, AND GRANTING DAMAGES AND PERMANENT INJUNCTIVE RELIEF

Defendant Power Ventures, Inc. ("Power Ventures") and Defendant Steve Vachani ("Vachani") (collectively,

"Defendants") request leave to file a motion for reconsideration of the February 16, 2012 summary judgment order issued by Judge James Ware. Plaintiff, Facebook, Inc. moves for statutory and compensatory damages, permanent injunctive relief, and a grant of summary judgment holding that Vachani is personally liable for violations of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C § 7701; the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; and California Penal Code § 502. Pursuant to Civil Local Rule 7-1(b), the Court finds a hearing unnecessary for resolution of these matters and accordingly VACATES the hearing and case management conference set for September 26, 2013. Having considered Defendants' papers and the record in this case, Defendants' request for leave to file a motion for reconsideration is DENIED. Plaintiff's motion for statutory and compensatory damages, motion for permanent injunctive relief, and motion for summary judgment on the issue of Vachani's personal liability are GRANTED. The Court proceeds to discuss each issue in turn.

I. BACKGROUND

A. Factual Background

Facebook owns and operates the eponymous social networking website located at facebook.com. First Amended Complaint ("FAC") ¶ 2. Power Ventures is a corporation incorporated in the Cayman Islands and doing business in California. Answer ¶ 10. It operates the

website www.power.com, which offers to integrate users' various social media accounts into a single experience. FAC ¶ 5; Answer ¶ 5. Vachani is the Chief Executive Officer of power.com. Answer ¶ 11.

Facebook brought this action against Defendants in December 2008, alleging violations of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C § 7701; the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; California Penal Code § 502; and the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201; copyright infringement under 17 U.S.C. § 101; trademark infringement under 15 U.S.C. §§ 1114 and 1125(a) and California law; and violations of California Business and Professions Code Section 17200. ECF Nos. 1, 9. Facebook complains that Defendants employ Facebook's proprietary data without its permission by inducing Facebook users to provide their login information and then using that information to "scrape" Facebook's proprietary material. FAC ¶¶ 49, 50, 52. Defendants then display Facebook's material on power.com. FAC ¶ 52. Facebook asserts that it never gave Defendants permission to use its material in this way. FAC ¶ 54.

Facebook also accuses Defendants of sending unsolicited and deceptive email messages to Facebook users. FAC ¶¶ 65-69. To launch their site, Defendants promised power.com users a chance to win $100 if they invited and signed up the most new users to Defendants' site. FAC ¶ 65. Defendants provided to their users a list of the users' Facebook friends from which the users could

choose people to whom to send the invitation. FAC ¶ 66. Power.com sent unsolicited commercial emails to those friends that included on the "from" line a "@facebookmail.com" address. FAC ¶¶ 66, 68. The content of the message included a line that the message was from "The Facebook Team." FAC ¶ 69, 70. Facebook contends that it never gave permission to send these messages and that the emails were deceptive because they "do not properly identify the initiators of the messages, nor do they provide clear or conspicuous notice that the messages are advertisements for" power.com. FAC ¶ 71.

B. Procedural Background

On February 18, 2011, Judge Ware granted the parties' stipulation to dismiss Facebook's DMCA claim, copyright and trademark infringement claims, and claims for violations of California Business and Professions Code Section 17200. ECF No. 97. On May 9, 2011, Defendants moved for summary judgment on Facebook's CFAA, Section 502, and CAN-SPAM Act claims. ECF No. 98. On November 17, 2011, Facebook moved for summary judgment on Facebook's § 502 and CFAA claims. ECF No. 214 ("§ 502/CFAA Motion"). On November 18, 2011, Facebook moved for summary judgment on Facebook's CAN-SPAM Act claim. ECF No. 215 ("CAN-SPAM Motion"). On February 16, 2012, Judge Ware issued an order denying Defendants' motion for summary judgment and granting summary judgment in Facebook's favor as to Facebook's § 502, CFAA, and CAN-SPAM Act claims. ECF No. 275 ("February 16 order").

Appendix C

In the February 16 order, Judge Ware requested additional briefing regarding Vachani's individual liability and the amount of damages Facebook should receive in light of the February 16 order. *Id.* at 19. On March 30, 2012, Facebook filed its supplemental brief regarding damages and the liability of Vachani. ECF No. 299 ("Facebook Damages/Liability Brief"). The same day, Defendants lodged with the court a brief regarding damages and the liability of Vachani. ECF No. 288 ("Defendants' Damages/Liability Brief"). On August 15, 2012, Vachani also submitted a supplemental brief regarding damages and his personal liability. ECF No. 317 ("Vachani Damages/Liability Brief").

On June 4, 2012, the attorneys representing Vachani and Power Ventures moved to withdraw as counsel. ECF Nos. 302, 303. On July 2, 2012, Judge Ware granted the motions to withdraw. ECF No. 306. In the order granting the withdrawal requests, Judge Ware required Vachani and Power Ventures to file Notices of Identification of Substitute Counsel no later than July 17, 2012. *Id.* Judge Ware noted that although Vachani could proceed *pro se*, Power Ventures had to be represented by a member of the bar pursuant to Civil L.R. 3-9(b). *Id.* Judge Ware cautioned Defendants that a failure to file timely Notices of Identification of Substitute Counsel may result in default of the case. *Id.*

On July 19, 2012, after neither Vachani nor Power Ventures had filed a Notice of Identification of Substitute Counsel, Judge Ware ordered both parties to appear on August 6, 2012 to respond to an Order to Show Cause

regarding Defendants' failure to obtain counsel. ECF No. 308. On August 6, 2012, the parties appeared for the hearing, and on August 8, 2012, Judge Ware issued an order regarding Defendants' failure to obtain counsel ("August 8 order"). ECF No. 313. Because Power Ventures had failed to identify replacement counsel, Judge Ware found good cause to strike Power Ventures' answer to Facebook's complaint and enter default against Power Ventures. *Id.* Judge Ware permitted Vachani a short extension to find new counsel, which was conditioned on Vachani's immediate filing of a Notice of Self-Representation. *Id.* The Clerk entered default against Power Ventures on August 9, 2012. ECF No. 314.

On August 15, 2012, new counsel filed a Notice of Appearance on behalf of Power Ventures. ECF No. 316. That same day, Power Ventures moved for leave to file a motion for reconsideration of Judge Ware's August 8 order requiring entry of default against Power Ventures. ECF No. 318. Judge Ware gave Power Ventures leave to file the motion for reconsideration on August 21, 2012. ECF No. 320. On August 23, 2012, Power Ventures filed its motion for reconsideration. ECF No. 321. On August 27, 2012, Facebook filed its response and simultaneously requested entry of default judgment against Power Ventures. ECF No. 322.

On August 27, 2012, Defendants provided notice that both Power Ventures and Vachani had filed for bankruptcy. ECF Nos. 323, 324. Noting that pursuant to 11 U.S.C. § 362(a)(1), a voluntary petition for bankruptcy operates as an automatic stay of any judicial actions involving

the petitioners, Judge Ware stayed the proceedings and administratively closed the case on August 29, 2012. ECF No. 325. In the same order, Judge Ware denied as premature Power Ventures' motion for reconsideration of the August 8 order requiring entry of default. *Id.*

On March 20, 2013, Facebook notified the Court that the Bankruptcy Court had dismissed Power Ventures' bankruptcy case and had granted Facebook's request for relief from the automatic stay in Vachani's bankruptcy case. ECF No. 327. Facebook sought to reopen the case. *Id.* Facebook also sought reassignment to a new judge because on August 31, 2012, while the automatic stay was in effect, Judge Ware resigned from the bench. *Id.* On April 8, 2013, the undersigned judge, as the Duty Judge at the time Facebook filed its motion, granted Facebook's request. ECF No. 328. The undersigned judge ordered that the stay be lifted, the case be reopened, and the case be reassigned. *Id.* The case then was reassigned to the undersigned judge. ECF No. 329.

On April 25, 2013, Vachani moved for clarification of the February 16 order regarding whether Vachani's liability had been determined in the February 16 order. ECF No. 332. On April 29, 2013, Facebook filed a case management statement in which Facebook again requested that default judgment be entered against Power Ventures. ECF No. 333. On the same day, Defendants filed a consolidated case management statement in which Power Ventures again sought to set aside default. ECF No. 334. Defendants also stated their intent to request leave to file a motion for reconsideration of the February 16

order. *Id.* In Facebook's and Defendants' respective case management statements, the parties acknowledged that Vachani's liability and the issues of damages and injunctive relief still need to be addressed. ECF No. 333, 334.

On May 2, 2013, following a case management conference, the Court issued a case management order. ECF No. 340. In that order, the Court clarified that the February 16 order did not decide Vachani's liability. *Id.* The Court granted Power Ventures' request to set aside default and denied Facebook's request for entry of default judgment against Power Ventures. *Id.* The Court also set a briefing schedule for the damages and injunctive relief issues. *Id.* The Court set a hearing date of September 26, 2013 to consider Vachani's liability, as well as the remedies issues. *Id.*

On August 1, 2013, Power Ventures filed its request for leave to file a motion to reconsider the February 16 order. ECF No. 353. On August 1, 2013, Facebook filed its supplemental memorandum in support of its request for injunctive relief. ECF No. 354 ("Facebook Injunction Brief"). On August 15, 2013, Defendants filed a response to Facebook's request for injunctive relief. ECF No. 357 ("Defendants' Inj. Opp.") On August 22, 2013, Facebook filed its reply. ECF No. 358 ("Facebook Injunction Reply").[1]

1. Vachani has appealed Magistrate Judge Joseph Spero's order granting Facebook fees and costs for Vachani's second Rule 30(b)(6) deposition, which Judge Spero granted because of Defendants' misconduct during discovery. ECF No. 356 (Order granting fees); ECF No. 360 (Notice of Appeal by Vachani). Vachani's

Appendix C

II. LEGAL STANDARDS

A. Motion for Reconsideration

Pursuant to Civil Local Rule 7-9, "[b]efore the entry of a judgment adjudicating all of the claims and the rights and liabilities of all the parties in a case, any party may make a motion before a Judge requesting that the Judge grant the party leave to file a motion for reconsideration of any interlocutory order made by that Judge on any ground set forth in Civil L.R. 7-9(b). No party may notice a motion for reconsideration without first obtaining leave of Court to file the motion." Civil Local Rule 7-9(b) provides three grounds for reconsideration of an interlocutory order:

> (1) That at the time of the motion for leave, a material difference in fact or law exists from that which was presented to the Court before entry of the interlocutory order for which reconsideration is sought. The party also must show that in the exercise of reasonable diligence the party applying for reconsideration did not know such fact

---

appeal does not divest this Court of jurisdiction over the issues resolved in this order because the filing of a notice of appeal divests the district court of jurisdiction only over the matters appealed. *Masalosalo by Masalosalo v. Stonewall Ins. Co.*, 718 F.2d 955, 956 (9th Cir. 1983) ("A notice of appeal only transfers jurisdiction to the appellate court over matters contained in the appeal."); *Donovan v. Mazzola*, 761 F.2d 1411 (9th Cir. 1985) ("Appeal of one order does not necessarily deprive the district court of jurisdiction over issues not raised in that order.").

or law at the time of the interlocutory order; or

(2) The emergence of new material facts or a change of law occurring after the time of such order; or

(3) A manifest failure by the Court to consider material facts or dispositive legal arguments which were presented to the Court before such interlocutory order.

Rule 7-9(c) further requires that "[n]o motion for leave to file a motion for reconsideration may repeat any oral or written argument made by the applying party in support of or in opposition to the interlocutory order which the party now seeks to have reconsidered." In general, motions for reconsideration should not be frequently made or freely granted. *See generally Twentieth Century- Fox Film Corp. v. Dunnahoo*, 637 F.2d 1338, 1341 (9th Cir. 1981).

B. Summary Judgment Regarding Liability of Vachani

Summary judgment is appropriate if, viewing the evidence and drawing all reasonable inferences in the light most favorable to the nonmoving party, there are no genuine disputed issues of material fact, and the movant is entitled to judgment as a matter of law. FED. R. CIV. P. 56(a); *Celotex v. Catrett*, 477 U.S. 317, 322, 106 S. Ct. 2548, 91 L. Ed. 2d 265 (1986). A fact is "material" if it "might affect the outcome of the suit under the governing law," and a dispute as to a material fact is "genuine" if

there is sufficient evidence for a reasonable trier of fact to decide in favor of the nonmoving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 106 S. Ct. 2505, 91 L. Ed. 2d 202 (1986). "If the evidence is merely colorable, or is not significantly probative," the court may grant summary judgment. *Id.* at 249-50. (citation omitted). At the summary judgment stage, the Court "does not assess credibility or weigh the evidence, but simply determines whether there is a genuine factual issue for trial." *House v. Bell*, 547 U.S. 518, 559-60, 126 S. Ct. 2064, 165 L. Ed. 2d 1 (2006).

The moving party has the burden of demonstrating the absence of a genuine issue of fact for trial. *Celotex*, 477 U.S. at 323. It "must either produce evidence negating an essential element of the nonmoving party's claim or defense or show that the nonmoving party does not have enough evidence of an essential element to carry its ultimate burden of persuasion at trial." *Nissan Fire & Marine Ins. Co. v. Fritz Companies, Inc.*, 210 F.3d 1099, 1102 (9th Cir. 2000) (citation omitted). Once the moving party has satisfied its initial burden of production, the burden shifts to the nonmoving party to show that there is a genuine issue of material fact. *Id.* at 1103.

C. Permanent Injunctive Relief

A party seeking a permanent injunction must make a four-part showing: (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by

a permanent injunction. *See eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 390, 126 S. Ct. 1837, 164 L. Ed. 2d 641 (2006).

III. ANALYSIS OF DEFENDANTS' MOTION FOR RECONSIDERATION

Defendants proffer three grounds in support of their request for reconsideration, notably none of which arise out of a material difference in fact or law either at the time the February 16 order was issued or in the intervening period. Defendants instead assert that the February 16 order represents a "manifest failure" to consider "material facts or dispositive legal arguments which were presented" and that the order includes "conclusions of law counter to precedent controlling authorities." Mot. Recons. at 2. In support of their position, Defendants argue that (1) the February 16 order incorrectly applied the law by finding that the email messages were materially misleading; (2) the order incorrectly considered the issue of data ownership under the CFAA and § 502 claims; and (3) the order incorrectly classified Facebook's damages in determining that Facebook had standing to litigate its claims. Mot. Recons. at 3.

A. Materially Misleading Emails

Defendants argue that the February 16 order incorrectly applied the law by finding that the email messages Defendants caused to be sent to Facebook users were materially misleading. Defendants assert that the header information was not materially misleading because

within the body of the email, Defendants were identified and because no one complained about being misled. Mot. Recons. at 3-4.

To establish liability under the CAN-SPAM Act, Facebook had to establish that Defendants' emails were materially misleading. 15 U.S.C. § 7704(a)(1). The Act provides that "[i]t is unlawful for any person to initiate the transmission, to a protected computer of a commercial electronic mail message . . . that contains, or is accompanied by, header information that is materially false or materially misleading." *Id.* The Act defines "materially" "when used with respect to false or misleading header information" to include:

> the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

15 U.S.C. § 7704(a)(6).

Defendants' arguments fail to meet the standard for reconsideration for three reasons. First, Defendants presented essentially the same arguments to Judge Ware in their opposition to Facebook's CAN-SPAM Motion.

ECF No. 239. In Defendants' opposition to the CAN-SPAM Motion, Defendants asserted that the header information was not materially misleading because Facebook in fact had generated the emails and because no one complained about being misled. ECF No. 239 at 11-12. The significant overlap in the arguments alone warrants denial of Defendants' request. Moreover, to the extent Defendants failed to present these arguments in Defendants' opposition to Facebook's CAN-SPAM Motion, Defendants have provided no reason why they could not have done so at that time.

Second, Judge Ware considered Defendants' arguments in his order. In the February 16 order, Judge Ware addressed whether the "from" line in the emails rendered the emails materially misleading as required under the CAN-SPAM Act. ECF No. 275 at 13. Judge Ware also addressed Defendants' argument that the body of the email corrected any misrepresentation in the header information. *Id.* Judge Ware therefore did not manifestly fail to consider Defendants' legal theories or material facts.

Third, Judge Ware's consideration of Defendants' argument was not clear error. The February 16 order correctly states that a false or misleading statement is considered material if "the alteration or concealment of header information" would impair the ability of an Internet Service Provider ("ISP") or the recipient of the email to "identify, locate, or respond to a person who initiated the electronic mail message." 15 U.S.C. § 7704(a)(6). The parties did not dispute that the "from"

line of the emails Defendants caused to be sent listed the address "@facebookmail.com." ECF No. 375 at 13. Judge Ware found that the "@facebookmail.com" failed to provide the recipient with an ability to identify, locate, or respond to Defendants. ECF No. 275 at 13. As a result, Judge Ware concluded that the headers were materially misleading as defined by the statute. *Id.* Judge Ware did not, as Defendants argue, hold that misleading header information is a per se violation of the CAN-SPAM Act.

Defendants have failed to meet their burden for leave to request reconsideration of the February 16 order on this issue.

B. Violations Under the CFAA and § 502

Defendants next argue that reconsideration of the February 16 order is warranted because Judge Ware failed to address whether the information Defendants took from Facebook had value. Mot. Default J. at 4-5. Defendants assert that a determination of value was necessary because violations under the CFAA and § 502 require a showing that the taken information had value. *Id.* The Court first addresses Defendants' CFAA argument.

Appendix C

The CFAA prohibits several types of activities involving fraud and unauthorized access to protected computers. 18 U.S.C. § 1030(a)(1)-(7). The CFAA provides a civil cause of action for a violation of any of its provisions. Specifically, the CFAA provides that "[a]ny person who suffers damage or loss by reason of a violation of this section [i.e. Section 1030] may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

Notably, the CFAA defines "loss" and "damage" separately from the actions prohibited under the CFAA. *See* 18 U.S.C. § 1030(a)(1)-(7) (describing prohibited activities); § 1030(e)(8) (defining "damage"); § 1030(e) (11) (defining "loss"). The Court addresses in this section only the violations of the CFAA that serve as the basis of Facebook's CFAA cause of action and addresses the "damage or loss" requirement in Section C below.

In Facebook's § 502/CFAA Motion, Facebook alleged that Defendants had violated both 18 U.S.C. § 1030(a)(2)(C) and 18 U.S.C. § 1030(a)(4). Either violation could serve as the basis for Facebook's CFAA cause of action. Section 1030(a) (2)(C) prohibits a person from "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." Section 1030(a)(4) meanwhile prohibits a person from:

> knowingly and with intent to defraud, access[ing] a protected computer without authorization, or

> exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

Notably, while Section 1030(a)(4) prohibits unauthorized access to a protected computer that results in obtaining "anything of value," Section 1030(a)(2)(C) prohibits unauthorized access that results in obtaining only "information." Thus, Section 1030(a)(2)(C) does not require a showing that the taken information had value.

In the February 16 order, Judge Ware determined that Defendants had violated Section 1030(a)(2)(C). ECF No. 275 at 17-18. In his analysis, Judge Ware found that an admission by Defendants that Defendants had taken, copied, or used data from Facebook's site established that Defendants had "obtain[ed] information" from Facebook, as required to establish a violation under Section 1030(a) (2)(C). ECF No. 275 at 18. Because Judge Ware found a violation of the CFAA under Section 1030(a) (2) (C), Judge Ware did not need to address Facebook's alternative argument that Defendants had also violated Section 1030(a)(4), which would require a showing that the taken information had value. Accordingly, as Defendants correctly point out, Judge Ware in the February 16 order did not explicitly analyze whether the taken information had value. Thus, Defendants' argument is meritless. Defendants have not shown that Judge Ware manifestly

failed to consider a dispositive legal argument or that Judge Ware clearly erred.

Defendants' arguments regarding § 502(c) likewise are unavailing. Section 502(c) prohibits, among other things, a person from "knowingly access[ing] and without permission tak[ing], cop[ying] or ma[king] use of any data from a computer, computer system or computer network." Cal. Penal Code § 502(c)(2). Section 502(e)(1) confers standing for a civil cause of action on an "owner or lessee of the . . . data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c)." In Section C below, the Court addresses the "damage or loss" requirement.

Judge Ware determined that Defendants' admission established that Defendants had violated § 502(c), and Judge Ware further determined that Facebook had suffered a loss as a result of that violation. ECF No. 275 at 14-15; ECF No. 89 at 8. As with Section 1030(a)(2)(C) of the CFAA, the plain language of § 502(c) does not require that any data that was taken be valuable. Defendants offered no case law in their opposition to Facebook's § 502/CFAA Motion and do not offer any case law in this motion suggesting that § 502(c) requires that the data that was taken be valuable. *See* ECF No. 242 at 4-5; Mot. Default. J. at 5. Thus, Defendants have not shown that Judge Ware's finding that Defendants were liable under § 502(c) reflects a manifest failure to consider a dispositive legal theory or clear error.

Defendants also include a new argument in the motion for leave to seek reconsideration that because Defendants did not destroy any information or data Defendants are not liable under the CFAA or § 502.[2] Mot. Default J. at 5. Nothing in the plain language of either Section 1030(a)(2) (C) or § 502 requires that taken information be destroyed, and Defendants do not point to any case law suggesting otherwise. Furthermore, Defendants do not explain why Defendants did not or could not raise the new argument in their opposition to Facebook's § 502/CFAA Motion. The Court thus finds Defendants' new argument is not grounds for leave to request reconsideration.

C. Standing

Defendants finally argue that Judge Ware erred in finding that Facebook had established sufficient harm to have standing under the CAN-SPAM Act, § 502, and the CFAA. Mot. Recons. at 5-6. Defendants have not made the requisite showing to justify reconsidering the February 16 order.

---

2. Defendants also assert that Facebook never had ownership over the information and that the information did not have proprietary value. Mot. Recons. at 5. The Court finds these arguments to be duplicative of arguments that Defendants presented to Judge Ware in their opposition to Facebook's Section 502/CFAA Motion. The Court thus finds these arguments do not constitute grounds for leave to seek reconsideration.

Appendix C

1. CAN-SPAM Act

To recover under the CAN-SPAM Act, Facebook had to establish that it was "adversely affected by a violation of . . . or a pattern or practice that violates" the Act. 15 U.S.C. § 7706(g)(1). In *Gordon v. Virtumundo, Inc.*, the Ninth Circuit held that to be "adversely affected" under the CAN-SPAM Act, an ISP must experience harm that is "both real and the type experienced by ISPs." 575 F.3d 1040, 1053 (9th Cir. 2009).

In this motion, Defendants argue that Facebook's harm evidence fails to meet the standard under *Gordon*. Defendants' argument, however, is recycled from the argument Defendants made before Judge Ware in opposition to Facebook's CAN-SPAM Motion. In their opposition to the CAN-SPAM Motion, Defendants argued that under *Gordon* Facebook's claimed injuries do not give rise to standing under the statute. ECF No. 239 at 14-15. Defendants repeat that argument in this motion. Accordingly, Defendants have not established that leave for reconsideration is warranted.

The Court further finds that Judge Ware considered Defendants' argument in the February 16 order. In his order, Judge Ware addressed *Gordon* and concluded that Facebook's evidence of costs incurred as a result of investigating Defendants' unauthorized access and the legal fees incurred in trying to stop Defendants' unauthorized access sufficed to confer standing on Facebook under the CAN-SPAM Act. ECF No. 275 at 8-9. The analysis of *Gordon* and Facebook's evidence in the

February 16 order precludes any claim by Defendants that Judge Ware manifestly failed to address either material facts or legal arguments. *See id.*

There is no clear error or manifest injustice in Judge Ware's analysis. The February 16 order describes how Facebook's evidence of injury from having to address Defendants' unauthorized access amounts to the type of specialized harm against which the CAN-SPAM Act protects. ECF No. 275 at 7-8. *Gordon* advises that "the threshold of standing should not pose a high bar for the legitimate service operations contemplated by Congress" in instituting the CAN-SPAM Act, and so for "well-recognized ISPs or plainly legitimate [ISPs] . . . adequate harm might be presumed." 575 F.3d at 1055. In light of that advice, the Court finds no clear error or manifest injustice in Judge Ware's holding.

2. CFAA and § 502

In this motion, Defendants argue that the costs Facebook incurred from investigating Defendants' actions and having Facebook's attorneys respond to Defendants' activities are insufficient to show harm under the CFAA and § 502.

The CFAA defines "loss" as:

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition

> prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]

18 U.S.C. § 1030(e)(11).

§ 502(e)(1) in turn provides that:

> the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access.

§ 502 does not further define "loss."

Defendants' argument in support of its request for leave to move for reconsideration is unavailing. First, Defendants raised this argument in the opposition to Facebook's § 502/CFAA Motion. ECF No. 242 at 11. To the extent Defendants repeat arguments from their opposition to the § 502/CFAA Motion, Defendants have not established grounds for seeking reconsideration. Defendants add new case law in this motion, but Defendants offer no reasons why they did not or could not present these decisions in Defendants' opposition to Facebook's § 502/CFAA Motion.

Second, Judge Ware addressed Defendants' arguments regarding harm under the CFAA and § 502. Judge Ware specifically determined that the costs Facebook incurred to block Defendants from the site, to investigate Defendants' activities, and to have its attorneys attempt to stop Defendants from continuing the activities were sufficient to establish loss under the CFAA and § 502. ECF No. 275 at 18; ECF No. 89 at 8. Defendants therefore cannot assert that the order reflects a manifest failure to consider either material facts or dispositive legal arguments.

Third, the Court finds no manifest injustice or clear error in the February 16 order regarding Facebook's "loss" under the CFAA or § 502. Given that the CFAA explicitly identifies the "cost of responding to an offense" and "conducting a damage assessment" as types of losses for which the CFAA confers standing, the Court finds no clear error in Judge Ware's determination that Facebook's costs meet the definition of "loss" provided by the CFAA. *See Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010) ("Costs associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute."). The Court also finds that Judge Ware's determination that Facebook's costs satisfy the "loss" requirement under § 502 is not clear error. *See Yee v. Lin*, No. C 12-02474 WHA, 2012 U.S. Dist. LEXIS 134936, 2012 WL 4343778, at *3 (N.D. Cal. Sept. 20, 2012) (finding that plaintiff's expenses "associated with responding" to defendant's unauthorized access were sufficient to meet loss requirement under § 502).

The Court further finds no manifest injustice or clear error in the February 16 order based on Defendants' late-added case law. *See AtPac, Inc. v. Aptitude Solutions, Inc.*, 730 F. Supp. 2d 1174, 1184 (E.D. Cal. 2010) (noting that under the CFAA, "[c]ognizable costs also include the costs associated with assessing a hacked system for damage"); *Farmers Insurance Exchange v. Steele Insurance Agency, Inc.*, No. 2:13-cv-00784-MCE-DAD, 2013 U.S. Dist. LEXIS 104606, 2013 WL 3872950, at *21 (E.D. Cal. July 25, 2013) (same).

Defendants have not established that leave to request reconsideration of the February 16 order is warranted.

IV. STEVEN VACHANI'S PERSONAL LIABILITY FOR VIOLATIONS OF THE CAN-SPAM ACT, CFAA, AND CALIFORNIA PENAL CODE § 502

The next issue before the Court is whether there is a genuine issue of material fact as to whether Defendant Steve Vachani, who was CEO of Power Ventures during the time period in question, is personally liable for statutory violations of the CAN-SPAM Act, CFAA, and California Penal Code § 502. For the reasons explained below, the Court concludes Vachani is personally liable as a matter of law and is thus jointly and severally liable with Power Ventures for violations of these statutory provisions.

Before analyzing Vachani's personal liability, the Court first summarizes this Court's previous findings regarding the precise conduct by Power Ventures that led to Judge Ware's finding of Power Venture's liability

under the CAN-SPAM Act, CFAA, and California Penal Code § 502. *See* ECF No. 275. The Court first held that Power Ventures, by creating the Launch Promotion and the software that caused Facebook's servers to send out the misleading emails with "@facebookmail.com" addresses to Facebook users, violated the provision of the CAN-SPAM Act which makes it unlawful "for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or misleading," 15 U.S.C. § 7704(a)(1). ECF No. 275 at 9-14. Second, the Court held that Power Ventures, by intentionally circumventing technical barriers to take, copy, or make use of data from the Facebook website without permission, violated California Penal Code § 502, which provides that a person is guilty of a public offense if he (1) knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network; (2) knowingly and without permission uses or causes to be used computer services; or (3) knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. California Penal Code §§ 502(c)(2),(3) & (7). ECF No. 275 at 14-17. Third, the Court held that Power Ventures, by accessing Facebook without authorization, and obtaining information from the Facebook website, violated the provision of CFAA that imposes liability on any party that "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," 18 U.S.C. § 1030(a)(2)(C). ECF No. 275 at 17-19.

Appendix C

The Court must decide whether Vachani should be held personally liable for violating these statutory provisions. The Ninth Circuit has held that "a corporate officer or director is, in general, personally liable for all torts which he authorizes or directs or in which he participates, notwithstanding that he acted as an agent of the corporation and not on his own behalf." *Comm. for Idaho's High Desert, Inc. v. Yost*, 92 F.3d 814, 823 (9th Cir. 1996) (quoting *Transgo, Inc. v. Ajac Transmission Parts Corp.*, 768 F.2d 1001, 1021 (9th Cir. 1985)). "Cases which have found personal liability on the part of corporate officers have typically involved instances where the defendant was the 'guiding spirit' behind the wrongful conduct, . . . or the 'central figure' in the challenged corporate activity." *Davis v. Metro Productions, Inc.*, 885 F.2d 515, 523 n.10 (9th Cir. 1989). Under such circumstances, both the corporation and the officers or directors who participated in the tortious conduct may be held liable. *See Moseley v. U.S. Appliance Corp.*, 155 F.2d 25, 27 (9th Cir. 1946). Thus, where an officer authorized, directed, or participated in a corporation's tort or statutory violation, the officer can be held personally liable. *See United States v. Reis*, 366 Fed. Appx. 781, 782 (9th Cir. 2010) (finding personal liability where corporate officer was an active participant in the acts giving rise to corporate liability under the Resource Conservation and Recovery Act); *Dish Network, LLC v. Sonicview USA, Inc.*, 2012 U.S. Dist. LEXIS 75663, 2012 WL 1965279, at *11 (S.D. Cal. May 31, 2012), *reconsideration denied*, 2012 U.S. Dist. LEXIS 134867, 2012 WL 4339047 (finding personal liability of several corporate officers who were the "guiding spirits" of the corporation's statutory violations of the Digital Millennium Copyright Act and the Federal Communications Act).

In this case, the Court must assess whether there is a genuine issue of material fact as to whether Vachani directed and authorized the specific activities giving rise to Power Ventures' liability to a degree that reflects more than simply his supervisory role as CEO of the company. More specifically, the Court assesses whether he was a "guiding spirit" or "central figure" in Power Venture's unlawful access to and use of the Facebook website.[3] *Davis*, 885 F.2d at 523 n.10. Again, the unlawful activities that led to Power Venture's liability under the three relevant statutes were 1) creating the Launch Promotion and the software that caused Facebook's servers to send out the misleading emails to Facebook users; 2) circumventing technical barriers to take, copy, or make use of data from the Facebook website without permission; 3) accessing Facebook without authorization and obtaining information from the Facebook website without authorization. ECF No. 275 at 9-19. Drawing all reasonable inferences in the light most favorable to Vachani, the Court concludes that the undisputed facts prove that Vachani authorized and directed these activities.

---

3. The Court notes that Facebook does not argue an alter ego theory; namely, it does not ask the Court to pierce the corporate veil in order to hold Vachani liable. In any event, courts have held that where officers direct, order, or participate in the company's tortious conduct, there is no need to pierce the corporate veil to establish the personal liability of the corporate officer. *Chase Inv. Servs. Corp. v. Law Offices of Jon Divens & Assocs.*, 748 F. Supp. 2d 1145, 2010 WL 4056022, at *28 (C.D.Cal. 2010) ("This principle applies regardless of the piercing of the corporate veil.")

Appendix C

First, with respect to the creation of the Launch Promotion[4] and the software through which Power Ventures caused Facebook's servers to send out the misleading emails to Facebook users, Vachani admitted he was "controlling and directing [Power's] activities as it related to Facebook," including "controlling and directing the activities related to the use of the Power 100 campaign in conjunction with Facebook users." ECF No. 299-3 at 27. Vachani also admitted that the Power 100 Campaign was his very own idea, ECF No. 229 at 7, and Defendants admit he managed the campaign's implementation. ECF No. 232-2 at 5-6 (Power Venture's Response to Interrogatories, noting Vachani was the "director responsible for developing the technology to allow Power or Power users to continue to access the Facebook website following Facebook's IP blocking" and for "creating the email messages sent to Facebook users asking Facebook users to use the Power website to access the Facebook website").[5] Given these admissions,

4. Around December 2008, Power Ventures began integrating with Facebook by allowing users to enter their Facebook account information and access the Facebook site through Power.com. FAC ¶ 49-50; Answer ¶ 49-50. Later, Power Ventures initiated a "Launch Promotion," or the Power 100 Campaign, that promised Power Venture's users the chance to win a $100 award if they invited and signed up new users. FAC ¶ 65; Answer ¶ 65. Power Ventures gave existing users a list of their Facebook friends Power Ventures had obtained from Facebook, and users had to select the friends who would receive a Power Ventures invitation, which would contain a "@facebookmail.com" sender address. *Id.* ¶66-68; *Id.* ¶ 66-68.

5. Defendants also admitted to the court in other papers that Vachani has "been personally involved in all of Power's operations including the Facebook integration that occurred in December 2008

the Court finds there is no genuine dispute regarding whether Vachani actually led the effort to create the Launch Promotion and to develop the software behind Power Venture's illegal actions.

Second, with respect to Power Venture's circumvention of Facebook's technical barriers to take, copy, or make use of data from the Facebook website without permission, the undisputed facts show that Vachani anticipated Facebook's attempts to block Power Venture's access and oversaw the implementation of a system that would be immune to such technical barriers so that Power Ventures could access Facebook's network. Vachani admitted that he directed the company's decision to circumvent Facebook's blocks of Power Venture's IP addresses. ECF No. 299-3 at 6-7 (Vachani deposition in which he admits he "was the person making the executive decision . . . to ensure that Facebook could not block Power.com"); ECF No. 299-3 at 28-29 (Vachani deposition admitting he controlled and directed employees' activities related to ensuring that Power Ventures continued to have access to Facebook); *see also* ECF No. 232-2 at 5-6 (Power Venture's Response to Interrogatories noting that Vachani was the "director responsible for developing the technology to allow Power or Power users to continue to access the Facebook website following Facebook's IP blocking"). There is also other evidence that Vachani instructed employees to circumvent the blocks he anticipated. ECF No. 236-6 at 2 (Email from Vachani to staff members stating that "we need to

---

that gave rise to this litigation." ECF No. 269 at 7 (response to Judge Joseph Spero regarding discovery dispute in this litigation).

be prepared for Facebook to try and block us . . ."); ECF No. 299-5 at 2 (Email from Vachani to employee noting, "please just make sure they cannot block us").[6]

Third, with respect to *obtaining* information from the Facebook website without authorization, Defendants admitted that they "took, copied, or made use of data from the Facebook website without Facebook's permission to do so." ECF No. 241-3 at 6 (Defendants' Reponses to Interrogatories). Vachani's admission that he controlled and directed "the activities related to the use of the Power 100 campaign in conjunction with Facebook users," ECF No. 299-3 at 27, suffices to show that there is no genuine dispute regarding whether he led the company's quest to obtain proprietary Facebook information, as that information was a necessary ingredient to the Power 100 Campaign. Ultimately, the Court concludes that these uncontroverted facts demonstrate Vachani was the "guiding spirit" behind Power Venture's efforts to send the misleading spam emails to Facebook users, and thus should be held personally liable.

Defendants' arguments to the contrary are unpersuasive. First, Defendants concede that corporate officers may be held liable for torts they authorize or direct, *see* Defendants' Damages/Liability Brief at 4-5, but claim that "corporate executives like Vachani

6. There is evidence that Vachani took other actions himself as well. ECF No. 299-3 at 8-9 (Vachani admitting he sent Facebook an email informing Facebook that Power Ventures would continue to try to access Facebook's services despite Facebook's request that the company stop).

cannot be held liable merely by virtue of their office for the torts of the corporation." *Id.* at 5. This argument neglects to take into consideration Vachani's specific acts with respect to the Power 100 Campaign that went above and beyond his merely advisory role as CEO of the company. Second, Defendants note that "there is no precedent for holding a CEO liable in this type of computer fraud and tort action where the CEO is not the exclusive owner or director . . ." Defendants' Inj. Opp. at 6. Vachani himself similarly argues he was never the sole owner, controlling shareholder, or controlling board member of Power Ventures, which he claims had six other executive officers and multiple board members who had significant influence in decision-making as well. *See* Vachani Damages/Liability Brief at 5-7, 15. It is true that the cases holding corporate officers personally liable for violations of CFAA, CAN-SPAM, or California Penal Code § 502 have involved factual situations in which the officer was either the *sole* officer or a majority shareholder of the company or some combination of both. *F.T.C. v. Sili Neutraceauticals, L.L.C.*, No. 07-C-4541, 2008 U.S. Dist. LEXIS 105683, 2008 WL 474116, at *3 (N.D. Ill. Jan. 23, 2008) (finding that sole officer of defendant corporation who formulated, directed, and controlled the acts giving rise to CAN-SPAM liability by the corporation was individually liable under CAN-SPAM); *Facebook v. Fisher*, No. C 09-05842, 2011 U.S. Dist. LEXIS 9668, 2011 WL 250395 (N.D. Cal. Jan. 26, 2011) (finding that sole officer of defendant corporation who conducted the acts giving rise to CAN-SPAM and CFAA liability by the corporation was individually liable under CAN-SPAM and CFAA); *Hanger Prosthetics & Orthotics, Inc., v. Capstone Orthopedic,*

Inc., 556 F. Supp. 2d 1122, 1134-35 (E.D. Cal. 2008) (denying motion for summary judgment on CFAA and California Penal Code § 502 claims against CEO where CEO owned one third of the corporation and a reasonable jury could infer that he authorized and directed the unlawful acts). However, Defendants fail to argue why an officer's majority shareholder status or sole officer position should make any difference to the liability outcome, especially given clear Ninth Circuit law in various other statutory contexts that holds corporate officers liable regardless of whether they are majority shareholders or sole officers. *See, e.g., Coastal Abstract Serv. Inc. v. First American Title Ins. Co.*, 173 F.3d 725, 734 (9th Cir. 1999) (holding officer of insurance company personally liable for violations of the Lanham Act despite the fact that he was acting as a corporate agent when committing the illegal conduct, without any discussion of his shareholder status). Accordingly, given the overwhelming evidence of Vachani's personal involvement in the unlawful acts leading to the statutory violations in this case, Defendants have failed to show that there is a genuine disputed issue of material fact concerning Vachani's personal liability, and the Court finds Vachani personally liable as a matter of law for violations of CAN-SPAM, CFAA, and California Penal Code § 502.

V. DAMAGES

In its memorandum in support of its request for injunctive relief, Facebook expressly waives its entitlement to attorneys' fees under the CFAA and its right to exemplary damages under California Penal Code

§ 502. Facebook Inj. Brief at 2.[7] However, Facebook seeks statutory damages under CAN-SPAM, asks the Court to treble damages, and also seeks compensatory damages under either CFAA or California Penal Code § 502. *Id.* at 1-13.

A. Facebook is entitled to damages under the CAN-SPAM ACT

Under the CAN-SPAM Act, a plaintiff may elect to recover monetary damages in an amount equal to the greater of actual losses or statutory damages. 15 U.S.C. § 7706(g)(1)(B). Facebook elects to recover statutory damages. It is well established that "[a] plaintiff may elect statutory damages regardless of the adequacy of the evidence offered as to his actual damages and the amount of the defendant's profits . . . and if statutory damages are elected, the court has wide discretion in determining the amount of statutory damages to be awarded, constrained only by the specified maxima and minima." *Facebook v. Wallace*, No. 09-798, 2009 U.S. Dist. LEXIS 107771, 2009 WL 3617789, at *2 (N.D. Cal. Oct. 29, 2009) (citation omitted) (internal quotations omitted). However, a statutory damages award may violate the due process rights of a defendant "where the penalty prescribed is so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable." *United States v. Citrin*, 972 F.2d 1044, 1051 (9th Cir. 1992) (citation omitted).

---

7. Facebook had previously requested punitive damages under Penal Code § 502. Facebook's Damages/Liability Brief at 10.

Appendix C

CAN-SPAM Act statutory damages are calculated as follows:

(3) Statutory damages.

(A) In general. For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message that is transmitted or attempted to be transmitted over the facilities of the provider of Internet access service, or that is transmitted or attempted to be transmitted to an electronic mail address obtained from the provider of Internet access service in violation of section 5(b)(1)(A)(i) [15 USCS § 7704(b)(1)(A)(i)], treated as a separate violation) by—

> (i) up to $ 100, in the case of a violation of section 5(a)(1) [15 USC § 7704(a)(1)]; or
>
> (ii) up to $ 25, in the case of any other violation of section 5 [15 USC § 7704].

(B) Limitation. For any violation of section 5 [15 USCS § 7704] (other than section 5(a)(1) [15 USC 7704(a)(1)]), the amount determined under subparagraph (A) may not exceed $ 1,000,000.

(C) Aggravated damages. The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if—

> (i) the court determines that the defendant committed the violation willfully and knowingly;
>
> or
>
> (ii) the defendant's unlawful activity included one or more of the aggravated violations set forth in section 5(b) [15 USC § 7704(b)].

15 U.S.C. § 7706(g)(3).

In this case, Facebook seeks to recover statutory damages pursuant to 15 U.S.C. § 7706(g)(3)(A)(i), which are calculated by multiplying the number of Header violations by up to $100.[8] The Court has already determined Defendants are liable for violating 15 U.S.C. § 7704(a)(1) because they initiated "a minimum of 60,000 instances of spamming." ECF No. 275 at 9. Facebook thus argues it is entitled to the maximum statutory damages of 100 dollars for each of the 60,627 spam messages Defendants sent to Facebook users. Facebook Damages/Liability Brief at 2. In its briefing, Defendants do not appear to contest the fact that they sent 60,627 email messages. Defendants' Damages/Liability Brief at 2-4. Facebook argues that the maximum is warranted because Defendants committed "egregious" actions by "designing their spamming campaign to ensure that it would continue notwithstanding any actions Facebook took to stop it" and "us[ing] cash payments to induce

8. Under the CAN-SPAM Act, each message is considered a separate violation. 15 U.S.C. § 7706(g)(3)(i).

third parties to send deceptive electronic messages." *Id.* at 2-3. Indeed, Defendants undisputedly utilized the incentive of monetary payments as a means to access Facebook users' accounts. FAC ¶¶ 66-70; Answer ¶¶ 66-70 (noting how Power's "Launch Promotion" offered site users 100 dollars if they successfully invited and signed up the most new Power.com users"). Defendants also undisputedly designed a system that would circumvent Facebook's blocking efforts. ECF No. 232-2 at 5-6 (Power Venture's Response to Interrogatories answering that they "develop[ed] the technology to allow Power or Power users to continue to access the Facebook website following Facebook's IP blocking").[9] Facebook also

9. Facebook also argues that Defendants' actions were "egregious" because they "destroyed evidence necessary to establish exactly how many messages, above the 60,627, they initiated." Facebook Damages/Liability Brief at 2-3. There is some evidence that Defendants did in fact delete evidence relevant to this lawsuit. Facebook's source code expert testified that a database called "Power_Logger" was one of two databases that should have recorded information about how many emails were sent to Facebook users throughout the Power 100 campaign. ECF No. 217 at ¶ 31-34. Defendants admitted that they deleted the Power_Logger database in April 2011. ECF No. 299-15 at 4-5 (Vachani admitting he made the decision to delete the database). *See also* ECF No. 220 at 12 (engineer's declaration in support of Facebook's opposition to Defendants' motion for summary judgment noting that "by deleting the Power_Logger database, Defendants effectively erased arguably the most relevant and useful information concerning the number of electronic mail messages that Defendants initiated through execution of their PowerScript software associated with the 100x100x100 campaign."); ECF No. 299-36 at 3 (Email from Defendants' counsel answering Plaintiff's counsel's request to identify the "missing databases related to the number of Launch Promotion messages that

asks the Court to treble the damages, contending that Defendants willfully and knowingly sent the deceptive spam messages to Facebook users. *Id.* at 8-9.[10] The record supports Facebook's contention that Defendants acted knowingly and willfully, *see e.g.* ECF No. 232-2 at 5-6 (Power's Response to Interrogatories answering that Vachani was "responsible for developing the technology to allow Power or Power users to continue to access the Facebook website following Facebook's IP blocking" and for "creating the email messages sent to Facebook users asking Facebook users to use the Power website to access the Facebook website").

In light of this evidence, the Court finds that a statutory damages award is warranted in this case. While Defendants argue that the Court should not award any damages under the CAN-SPAM Act because Facebook did not suffer "any specific harm" as a result of the email messages, citing *Gordon v. Virtumundo Inc.*, 575 F.3d 1040 (9th Cir. 2009), *see* Defendants' Damages/Liability Brief at 1-2, this argument fails for two reasons. First, this Court has already determined that under *Gordon*, Facebook has shown that it was "adversely affected" by

---

were sent to Facebook users" and stating that the Power_Logger database, which logs the activities on Power Venture's servers, has "missing tables" because Defendant chose not to back up those large files after it ceased operations and closed its server).

10. A court may treble damages under the CAN-SPAM Act where (1) the court determines that the defendant committed the violation willfully and knowingly; or (2) the defendant's unlawful activity included one or more of the aggravated violations in § 7704(b). 15 U.S.C. § 7706(f)(3)(C).

Defendants' actions within the meaning of the CAN-SPAM Act. ECF No. 275 at 8-9. Second, *Gordon* is inapposite here because it deals with whether a plaintiff has standing to bring a claim under the CAN-SPAM Act as opposed to whether the plaintiff deserves damages once liability under the Act has been determined, as in this case.[11] Nonetheless, exercising its broad discretion to determine an appropriate damages award, the Court finds that the $18,000,000 award requested by Facebook is unnecessary to address the deterrent and punitive purposes of a statutory damages award. Without deciding whether the requested $18,000,000 award would violate Defendants' due process rights, the Court declines to award that amount and finds it sufficient to award $50 per email communication that was sent. This decision is consistent with other cases where courts have declined to award the maximum statutory damages of $100 per violation, instead granting awards of either $50 or $25 per violation of the CAN-SPAM Act. *See Fisher*, 2011 U.S. Dist. LEXIS 9668, 2011 WL 250395 (awarding plaintiffs $50 per violation of the CAN-SPAM Act); *Wallace*, 2009 U.S. Dist. LEXIS 107771, 2009 WL 3617789 at *2 (same); *Tagged, Inc. v. Does 1 through 10*, No. C 09-01713, 2010 U.S. Dist. LEXIS 5428, 2010 WL 370331 (N.D. Cal. Jan. 25. 2010) (awarding plaintiffs only $25 for each of 6,079 spam emails in violation of CAN-SPAM Act in case

11. Defendant Vachani's own arguments against damages, namely that a damages decision could deter innovation and that "creating CAN-SPAM liability . . . would be unprecedented," are similarly unavailing. Vachani Damages/Liability Brief at 12-13. This Court has already found that he is liable, *see supra*, Part IV, and more importantly, damages, not liability, are at issue here.

where, unlike the instant case, *see supra* n.9, there was no evidence Defendants had actively deleted relevant database information to conceal the number of spam messages sent). Thus, Facebook will be granted $50 per email communication that was sent. It will be awarded $ 3,031,350 ($50 for each of the estimated 60,627 spam messages sent) in CAN-SPAM damages.

The Court also finds trebling unnecessary given the large size of the primary award amount. This finding is consistent with past cases where, despite defendants' willful and knowing violation of the statutes in question, courts refused to treble damages. *See Fisher*, 2011 U.S. Dist. LEXIS 9668, 2011 WL 250395 (holding that although defendants willfully and knowingly violated the statutes by engaging in the circumvention of Facebook's security measures, the requested maximum statutory award was disproportionate to the gravity of defendants' acts, and thus the court awarded plaintiffs $50 per violation and declined to treble damages); *Wallace*, 2009 U.S. Dist. LEXIS 107771, 2009 WL 3617789 at *2 (holding that although defendant "willfully violated the statutes in question with blatant disregard for the rights of Facebook and the thousands of Facebook users whose accounts were compromised by his conduct," and even violated a temporary restraining order and preliminary injunction, the requested maximum statutory award was not merited and the court awarded plaintiffs $50 per violation and declined to treble damages); *Tagged*, 2010 U.S. Dist. LEXIS 5428, 2010 WL 370331 (awarding $25 for each of 6,079 spam emails for a total amount of $151,975 and declining to treble damages because although

defendant's violations were allegedly intentional and willful, a $2,000,000 award was not justified).[12] Ultimately, a statutory damages award of $3,031,350 along with a permanent injunction which this Court grants, *see infra* Part VI, will adequately serve the purpose of punishment and deterrence in this case.

B. Facebook is entitled to compensatory damages under the CFAA

Under the CFAA, "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain

12. Facebook cites two default judgment orders in support of its request for $18,000,000. Facebook Damages/Liability Brief at 2-3. In *Facebook v. Guerbuez*, No. C 08-03889 (N.D. Cal. Nov. 21, 2008), Facebook was awarded $873 million against a defendant who sent four million spam emails to other Facebook users. In *Myspace v. Wallace*, 2008 U.S. Dist. LEXIS 75752 (C.D. Cal. May 28, 2008), Myspace was awarded $223 million against a defendant who had sent nearly 400,000 messages and posted 890,000 comments from 320,000 Myspace.com user accounts which were "hijacked." Here, in contrast, Defendants sent an estimated 60,627 individual emails. Accordingly, the Court concludes that it is just to award $3,031,350. Further, even if, as Facebook asserts, there are "tens of thousands of additional messages that Defendants littered through Facebook that cannot be accounted for in the damages calculation" due to Defendants' alleged destruction of the relevant database information, *see* Facebook Damages/Liability Brief at 6, the Court finds that a $3,031,350 award is sufficient, as courts in this district have granted awards proportionate to this award for similar violations. *See Tagged*, 2010 U.S. Dist. LEXIS 5428, 2010 WL 370331 (awarding plaintiff $151,975 for 6,079 emails that violated the CAN-SPAM Act where defendants' actions were intentional and willful and where defendant circumvented plaintiff's security measures like in this case).

a civil action against the violator to obtain *compensatory* damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g) (emphasis added). This Court previously held that Facebook suffered "loss" as a result of Defendants' violation of CFAA. ECF No. 275 at 18. Facebook is thus entitled to recover compensatory damages under the statute. Facebook has established through undisputed testimony[13] that it expended to investigate Defendants' actions and for outside legal services in connection with the Defendants' actions. Accordingly, this Court grants Facebook compensatory damages in the amount of $. Defendants' arguments against a grant of compensatory damages are unavailing. Defendants argue that Facebook "makes no effort to quantify any real harm it suffered" or "identify anything that Power misappropriated from Facebook's network." Defendants' Damages/Liability Brief at 3. Again, these arguments are irrelevant as they address issues on the merits that have already been decided; this Court previously found that Facebook *did* incur a "loss" under CFAA, and that Power Ventures *did* obtain information from Facebook without permission. ECF No. 275 at 18.[14]

---

13. This Court previously recognized that "Defendants do not dispute the accuracy or veracity of [the] evidence of [Facebook's] expenditures." ECF No. 275 at 8. Indeed, Defendants never filed a rebuttal brief to Facebook's expert report regarding the monetary damages Facebook incurred. ECF No. 299-26 (Expert Report of Richard Ostiller).

14. As the Court decides to grant Facebook compensatory damages under CFAA, the Court need not and does not analyze Facebook's alternative argument that Facebook deserves compensatory damages under California Penal Code Section 502(e) (1). Facebook's Damages/Liability Brief at 9.

Appendix C

VI. PERMANENT INJUNCTIVE RELIEF

Facebook moves for permanent injunctive relief to prevent future statutory violations by Defendants Vachani and Power Ventures. The CAN-SPAM Act authorizes the Court to grant a permanent injunction "to enjoin further violation by the defendant." 15 U.S.C. § 7706(g)(1)(A). Likewise, the CFAA provides that "[a]ny person who suffers damage or loss by reason of a violation of [§1030] may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C.A. § 1030(g). California Penal Code § 502 also allows a plaintiff to obtain injunctive relief. California Penal Code § 502(e)(1).

A party seeking a permanent injunction must make a four-part showing: (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction. *See eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 390, 126 S. Ct. 1837, 164 L. Ed. 2d 641 (2006). [15] The Court has discretion to grant or

15. Defendants cite Ninth Circuit law holding that when an injunction is sought to prevent the violation of a federal statute which specifically provides for injunctive relief, future violations are presumed once a statutory violation is shown and the standard requirements for equitable relief need not be satisfied before an injunction is granted. Facebook Inj. Brief at 6 (citing *Silver Sage Partners, LTD v. City of Desert Hot Springs*, 251 F.3d 814, 826-27

deny permanent injunctive relief. *Id.* at 391. The Court will consider each of these factors in turn, and will then consider whether, on balance, the principles of equity support the issuance of a permanent injunction in this case.[16]

(9th Cir. 2001) (Fair Housing Act context). The Court notes that although some courts have granted statutory injunctions in similar contexts without analyzing the traditional four factor test, *see Tagged*, 2010 U.S. Dist. LEXIS 5428, 2010 WL 370331(CFAA and California Penal Code §502); *Fisher*, 2011 U.S. Dist. LEXIS 9668, 2011 WL 250395 (CAN-SPAM Act and CFAA context), this Court declines to do so in light of Supreme Court authority reemphasizing the traditional four factor test. *See eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391-93, 126 S. Ct. 1837, 164 L. Ed. 2d 641 (2006) ("According to well established principles of equity, a plaintiff seeking a permanent injunction must satisfy a four-factor test before a court may grant such relief" and noting that the Supreme Court "has consistently rejected invitations to replace traditional equitable considerations with a rule that an injunction automatically follows a determination that a copyright has been infringed.")

16. Facebook objects to Vachani's declaration submitted in support of Defendants' Opposition to Injunctive Relief on the grounds that Vachani lacks personal knowledge for his various conclusions, including whether Facebook received any complaints about Defendants' conduct, and because he is not competent to testify regarding the various legal conclusions he makes, such as claiming "Power did not obtain [anything] . . . of value from Facebook." ECF No. 357-1; Facebook Injunction Brief at 2. For purposes of this Order only, the Court finds that Vachani's lack of qualifications and personal knowledge affect the weight his testimony should be accorded and not its admissibility. Thus, Facebook's objection is OVERRULED.

Appendix C

A. Irreparable Harm

Facebook has shown irreparable injury as a result of Defendants' violations of the law. Judge Ware's previous order granting Facebook summary judgment cited undisputed evidence that Defendants created a software program to access Facebook's website, scraped user information from Facebook, repeatedly changed Power Venture's IP address in order to circumvent technical barriers Facebook had installed, and used that information to cause Facebook's servers to send spam emails to Facebook users with "@facebookmail.com" mailing addresses. ECF No. 275 at 9-13. These activities constituted irreparable harm by harming Facebook's goodwill with its users because Facebook users receiving these emails are likely to associate the spam messages with Facebook. ECF No. 213 at ¶¶ 4-5. *Hotmail Corp. v. Van$ Money Pie Inc.*, 1998 U.S. Dist. LEXIS 10729, at *20-21 (N.D. Cal. Apr. 16, 1998) (holding that customer confusion from source of spam emails, which can lead to loss of goodwill, constituted irreparable harm to plaintiff); *Meineke Car Care Centers, Inc. v. Quinones*, 2006 U.S. Dist. LEXIS 40648, 2006 WL 1549708, *3 (W.D.N.C. 2006) (finding, in preliminary injunction context, that possible loss in customers resulting from defendants' deceptive suggestion that they were associated with plaintiff constituted irreparable harm). While Defendants argue that Facebook has not produced evidence that its reputation or goodwill with its users has been damaged as a result of Defendants' activities, *see* Defendants' Inj. Opp. at 5, 9, Defendants cite no case law suggesting that such specific and direct evidence is needed to prove harm

to goodwill. *C.f. Optinrealbig.com, LLC v. Ironport Sys., Inc.*, 323 F.Supp.2d 1037, 1050 (N.D. Cal. 2004) (emphasis added) ("Damage to a business' goodwill is typically an irreparable injury because it is *difficult to calculate*"); *see also Beacon Mut. Ins. Co. v. OneBeacon Ins. Group*, 376 F.3d 8, 17 (1st Cir. 2004) (rejecting argument that "only *direct* evidence (with no room for inference) may establish harm to goodwill" in the trademark law context).[17] As Facebook has shown irreparable harm, this factor weighs in favor of a permanent injunction.

B. Inadequacy of Money Damages

Facebook has established that "remedies available at law, such as monetary damages, are inadequate to compensate for [its] injury," *eBay*, 547 U.S. at 391, for three reasons. First, money damages will not ensure that Defendants will not take steps again in the future to spam Facebook users, which is a possibility. Defendants may still possess the software that enabled their illegal activities, and like in other cases in this district, Defendants also "deliberately implemented other tactics to circumvent plaintiff's security measures." *Tagged*,

17. Defendants also argue Facebook has not shown irreparable harm because Facebook has failed to submit proof of user complaints about the spam messages. Defendants' Inj. Opp. at 9. However, Facebook has provided evidence that in general, deceptive spam messages detract from Facebook user experiences and have been the source of complaints by Facebook users. ECF 218-8 at ¶ 5 (Declaration of Ryan McGeehan in support of Facebook's Motion for Partial Summary Judgment noting that "spam messages detract from the overall Facebook experience and are sometimes a source of complaints by Facebook users.

2010 U.S. Dist. LEXIS 5428, 2010 WL 370331, at *12. Defendants may even still possess Facebook-user data which they misappropriated. Because there is a "reasonable likelihood of defendant's future violations," injunctive relief is warranted. *Id.; Pyro Spectaculars North Inc. v. Souza*, 861 F.Supp.2d 1079, 1092 (E.D. Cal. March 21, 2012) (granting injunction in part because defendant still possessed plaintiff's data). Second, money damages will not compensate for the loss of goodwill Facebook may have suffered due to any confusion created by Defendants' emails. *See Hotmail*, 1998 U.S. Dist. LEXIS 10729 at *21 (holding that loss of goodwill caused by confusion generated by misleading spam emails "is not easily quantified and not adequately compensated with money damages."). Last, the Ninth Circuit has held that a district court has authority to issue an injunction "where the plaintiffs can establish that money damages will be an inadequate remedy due to impending insolvency of the defendant . . ." *In re Estate of Marcos*, 25 F.3d 1467 (9th Cir. 1994). Here, Defendants' voluntary petitions for bankruptcy, *see* ECF No. 323, 324, suggest they may be unable to satisfy a damages award and that non-monetary relief may be necessary.

In rebuttal, Defendants argue they never misappropriated Facebook user data. Defendants' Inj. Opp. at 8.[18] Defendants emphasize that one of their "primary" objections to injunctive relief is that "Defendants are not in possession of any Facebook data or any user data that was not expressly granted to Power by the users themselves."

18. *See also* Defendants' Inj. Opp. at 5 ("Facebook is unable to identify anything that Power misappropriated from Facebook's network, as Power did not take anything that belonged to Facebook.")

Id. at 3. This argument is irrelevant to the issue at hand because the Court has already ruled that Defendants did misappropriate data without Facebook's permission. ECF No. 275 at 14-18. Defendants also argue that the Court should not consider the fact that they may still possess the software that enabled the alleged violations because Power Ventures ceased operations in 2011. Defendants' Inj. Opp. at 8. But this argument ignores the fact that Defendants could easily start another company or give the data to other entities that wish to engage in the illegal spamming conduct.[19] Overall, as money damages will likely be inadequate, this factor weighs in favor of a permanent injunction.

C. Balance of Hardships

The balance of hardships analysis also weighs in favor of granting Facebook a permanent injunction. Defendants have been found liable for violating various laws, *see* ECF No. 275, and while an injunction would simply serve to force their compliance with the law, *see Myspace v. Wallace*, 498 F.Supp.2d 1293, 1306 (C.D. Cal. July 3, 2007) (holding defendant would experience no hardship if enjoined from committing further violations of the CAN-SPAM Act), Facebook may suffer harm if an injunction is not issued. As this Court previously concluded in its summary judgment order, Facebook has already suffered harm, as it incurred expenditures to both block Defendants' continued access

19. Defendants also argue that "damages were avoidable" because Defendants allegedly cooperated with Facebook through the litigation. Defendants' Inj. Opp. at 3, 10. This argument is irrelevant; the issue is not whether damages were "avoidable" but whether damages are sufficient to compensate Facebook for its injury.

to Facebook and to respond to the spamming emails. ECF No. 275 at 7-10. Absent an injunction Facebook may have to deal with future violations of the law. *Tagged*, 2010 U.S. Dist. LEXIS 5428, 2010 WL 370331, at *12 (granting a preliminary injunction against a defendant who violated CFAA and California Penal Code § 502 in part because defendant might engage in future violations). Indeed, Defendants have demonstrated a willingness to do so, as they did not stop even after requests from Facebook. ECF No. 299-3 at 8-9 (Vachani admitting that he sent Facebook an email informing Facebook that Power Ventures would continue to try to access Facebook's services despite Facebook's request that the company stop). On the other hand, Defendants claim that the requested injunction impermissibly threatens Vachani's employability and livelihood. Defendants' Inj. Opp. at 10-11; Vachani Damages/Liability Brief at 9. However, Defendants fail to provide a persuasive reason why this is the case, and in any event, given that Vachani brought this risk upon himself by violating the law, the balance would not shift in favor of Defendants even if there were evidence to support this speculative claim. Accordingly, the balance of hardships weighs in favor of Facebook.

D. Public Interest

The public interest weighs in favor of an injunction as well, and courts in this district have reached this conclusion in analogous cases. *See, e.g., Craigslist, Inc. v. Troopal Strategies, Inc.*, 2011 U.S. Dist. LEXIS 156825, at *11 (N.D. Cal. 2011) (holding injunction would be in the public interest where defendant violated CFAA). Injunctive relief would serve the public interest by preventing Defendants from impermissibly spamming

Facebook users again and setting an example to members of the public who may consider violating these various statutes as well. In passing the CAN-SPAM Act, Congress recognized the burdens which commercial spam poses to the public. 15 U.S.C. § 7701(a)(2) ("The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail."). Namely, the public "is forced to incur the costs of needlessly expended energy and time evaluating and eventually discarding defendants' unsolicited messages[.]" *F.T.C. v. Phoenix Avatar, LLC*, 2004 U.S. Dist. LEXIS 14717, 2004 WL 1746698, *14 (N.D. Ill. July 30, 2004) (enjoining defendants for violations of the CAN-SPAM Act). Because Defendants' activities fall within those activities Congress deemed detrimental to the public, this factor weighs in favor of Facebook. Defendants' arguments to the contrary are unavailing. While Defendants claim the injunction will pose "unacceptable risks for innovators" and enhancements in social networking technology, Defendants' Inj. Opp. at 11, this argument fails to recognize that the injunction will serve to deter only conduct that violates the law. The law explicitly provides for injunctive relief. Thus, to the extent that granting Facebook injunctive relief for Defendants' violations of CFAA and CAN-SPAM may have negative "impacts on innovation, competition, and the general 'openness' of the internet," courts have held that it is up to Congress, not the courts, to decide whether to amend those statutes. *Craigslist Inc. v. 3Taps*, No. CV 12-03816 CRB, 2013 U.S. Dist. LEXIS 116732, 2013 WL 4447520, at *25 (N.D. Cal. Aug. 16, 2013) ("[I]t is for Congress to weigh the significance of those consequences and decide whether amendment would be prudent.")

E. Balance of all four equitable factors

The balance of all four factors weighs strongly in favor of granting an injunction in this case. Thus, the Court grants Facebook its request for permanent injunctive relief against both Power Ventures and Vachani in his individual capacity.[20] This decision is in line with past decisions of this Court. *See Tagged*, 2010 U.S. Dist. LEXIS 5428, 2010 WL 370331, at *12 (granting injunctive relief for violations of CFAA and California Penal Code § 502); *Facebook v. Fisher*, 2011 U.S. Dist. LEXIS 9668, at *7-8 (N.D. Cal. Jan. 26. 2011) (granting injunction for violations of CAN-SPAM Act and CFAA); *Microsoft Corp. v. Neoburst Net LLC*, 2004 U.S. Dist. LEXIS 18733, at *2-4 (N.D. Cal. 2004) (granting injunctive relief for violations of CAN-SPAM Act, CFAA, and California Penal Code

20. While Defendants claim Facebook provides "no basis for enjoining the individual defendant from any action given that Vachani never acted independently or otherwise in a personal or individual capacity while employed by Power during the period of Facebook's grievances," Defendants' Inj. Opp. at 6, this argument fails for two reasons. First, as this Court finds that Vachani is personally liable, he may be enjoined in his individual capacity. *FTC v. Sili Neutraceuticals LLC*, 2008 U.S. Dist. LEXIS 105683 (N.D. Ill. Jan. 23, 2008). Second, even assuming this Court found Vachani was *not* personally liable, Defendants' argument ignores Ninth Circuit law holding that Federal Rule of Procedure 65 "establishes that an injunction may bind not only parties to the action but also 'their officers, agents, servants, employees, and attorneys, and [upon] those persons in active concert or participation with them.'" *Comedy Club Inc. v. Improv West Assocs.*, 553 F.3d 1277, 1287 (9th Cir. 2009) (citing FED. R. CIV. P. 65(d)). Here, Vachani may be enjoined under FRCP 65 as an officer of Power Venture.

§ 502).[21] Facebook is hereby entitled to a permanent injunction against Power Ventures and Vachani as follows:

1. Defendants, their agents, officers, contractors, directors, shareholders, employees, subsidiary companies or entities, affiliated or related companies and entities, assignees, and successors-in-interest, and those in active concert or participation with them, are permanently enjoined from:

A. Sending, or assisting others in the sending of, or procuring the sending of unauthorized or unsolicited commercial electronic text messages to users of the Facebook website, www.facebook.com, or via the Facebook website or service.

B. Making, or assisting others in making, any false or misleading oral or written statement or representation of material fact when advertising, promoting or selling any good or service, including, but not limited to any false or misleading statement or representation that Defendants, their representatives, or any other person is affiliated or associated with, under contract with, acting in partnership with, endorsed or approved by, or otherwise connected to Facebook or to a service offered by Facebook.

C. Accessing or using, or directing, aiding, facilitating, causing, or conspiring with others to use or access the Facebook website or servers for any purpose, without Facebook's prior permission.

---

21. Defendants' brief fails to distinguish or otherwise discuss these relevant authorities.

D. Using any data, including without limitation Facebook-user data and data regarding Facebook's website or computer networks, obtained as a result of the unlawful conduct alleged in the operative complaint in this action.

E. Developing, using, selling, offering for sale, or distributing, or directing, aiding, or conspiring with others to develop, sell, offer for sale, or distribute, any software that allows the user to engage in the unlawful conduct alleged in the operative complaint in this action.

2. Defendants, their agents, officers, contractors, directors, shareholders, employees, subsidiary companies or entities, affiliated or related companies and entities, assignees, and successors-in-interest, and those in active concert or participation with them shall destroy any software, script(s) or code designed to access or interact with the Facebook website, Facebook users, or the Facebook service. They shall also destroy Facebook data and/or information obtained from Facebook or Facebook's users, or anything derived from such data and/or information.

3. Within three calendar days of entry of this permanent injunction and order, Defendants shall notify their current and former officers, agents, servants, employees, successors, and assigns, and any persons acting in concert or participation with them of this permanent injunction.

4. Within seven calendar days of entry of this injunction and order, Defendants shall certify in writing, under penalty of perjury, that they have complied with the provision of this order.

5. The Court shall continue to retain jurisdiction over the parties for the purpose of enforcing this injunction and order.

VII. CONCLUSION

The Court finds Defendants have failed to set forth grounds pursuant to Civil L.R. 7-9(b) for leave to file a motion for reconsideration of Judge Ware's February 16 order. Thus, the request for leave is DENIED. The Court finds Vachani personally liable as a matter of law for violations of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C § 7701; the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; and California Penal Code § 502. The Court further finds Facebook is entitled to statutory damages in the amount of $3,031,350, compensatory damages in the amount of $, and permanent injunctive relief as described above. The Clerk shall close the file.

IT IS SO ORDERED.

Dated: September 25, 2013

/s/ Lucy H. Koh
LUCY H. KOH
United States District Judge